网络运维管理

第3讲：DNS实现

河南中医药大学信息技术学院
许成刚

一、DNS概述

1.DNS概述

- 在互联网访问时，如何获取目的主机的IP地址？
  - 例如访问河南中医药大学的WWW服务器，其IP地址是什么？
  - 记忆很多目的主机的IP地址是一件很困难的事，为了解决这些问题，互联网设计出域名系统（Domain name system，DNS）。域名系统可给机器分配用户名字（即域名），并且把这些名字与相应的IP地址关联起来。
  - 域名是比较容易记忆的，用户在访问某个互联网主机时，只需要输入其域名，则互联网的域名系统会自动解析出该域名对应的IP地址，并将其发给用户，接下来，用户的主机就可以通过IP地址访问目的主机了！
- 为了保证域名的唯一性，域名也需要申请和审批！

客户机如何才能获得百度的IP地址?

从表面来看，为了便于用户使用，互联网用户是通过域名www.baidu.com去访问百度服务器的，用户并不知道百度服务器的IP地址。

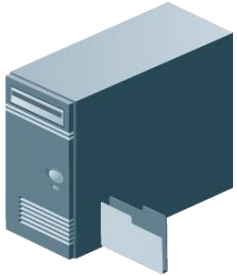
但实际上，用户主机必须知道百度服务器的IP地址，才能通过互联网（采用TCP/IP协议）访问到百度服务器。

如何解决上述的矛盾？

客户机如何才能获得百度的IP地址?

前面的例子中，当用户发出域名请求的时候（例如在浏览器中输入百度网址），该请求并不是直接发给百度服务器的，而是被互联网的域名系统（DNS）接收，DNS根据域名（www.baidu.com）解析出其对应的百度服务器的IP地址，并再此IP地址返回给用户，此时，用户就可以通过IP地址访问百度的服务器了。

DNS的基本解析过程

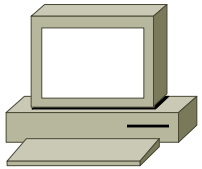


互联网的
DNS系统

客户机只知道百度的域名，
但不知道IP地址

?

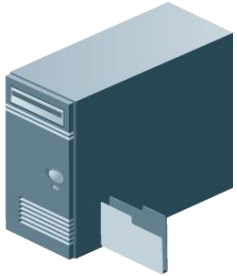
百度的Web服务器



访问：www.baidu.com

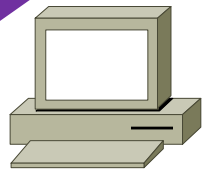
② 请求报文中包含待解析域名，
以UDP方式发给DNS系统

① 向DNS发送域名解析请求



互联网的
DNS系统

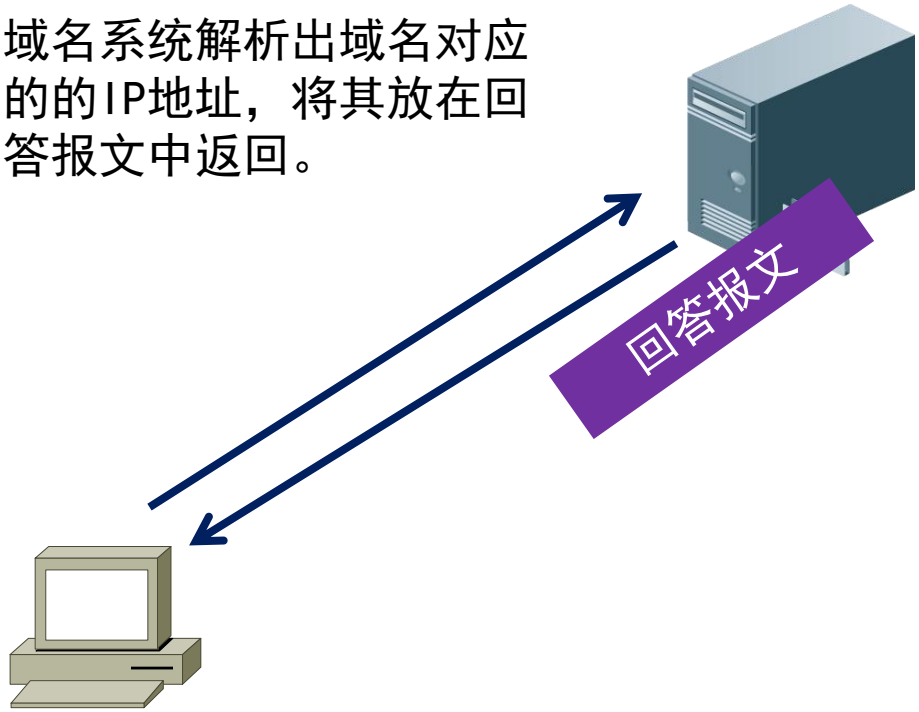
DNS请求报文



访问：www.baidu.com

Web服务器

③ 域名系统解析出域名对应的的IP地址，将其放在回答报文中返回。

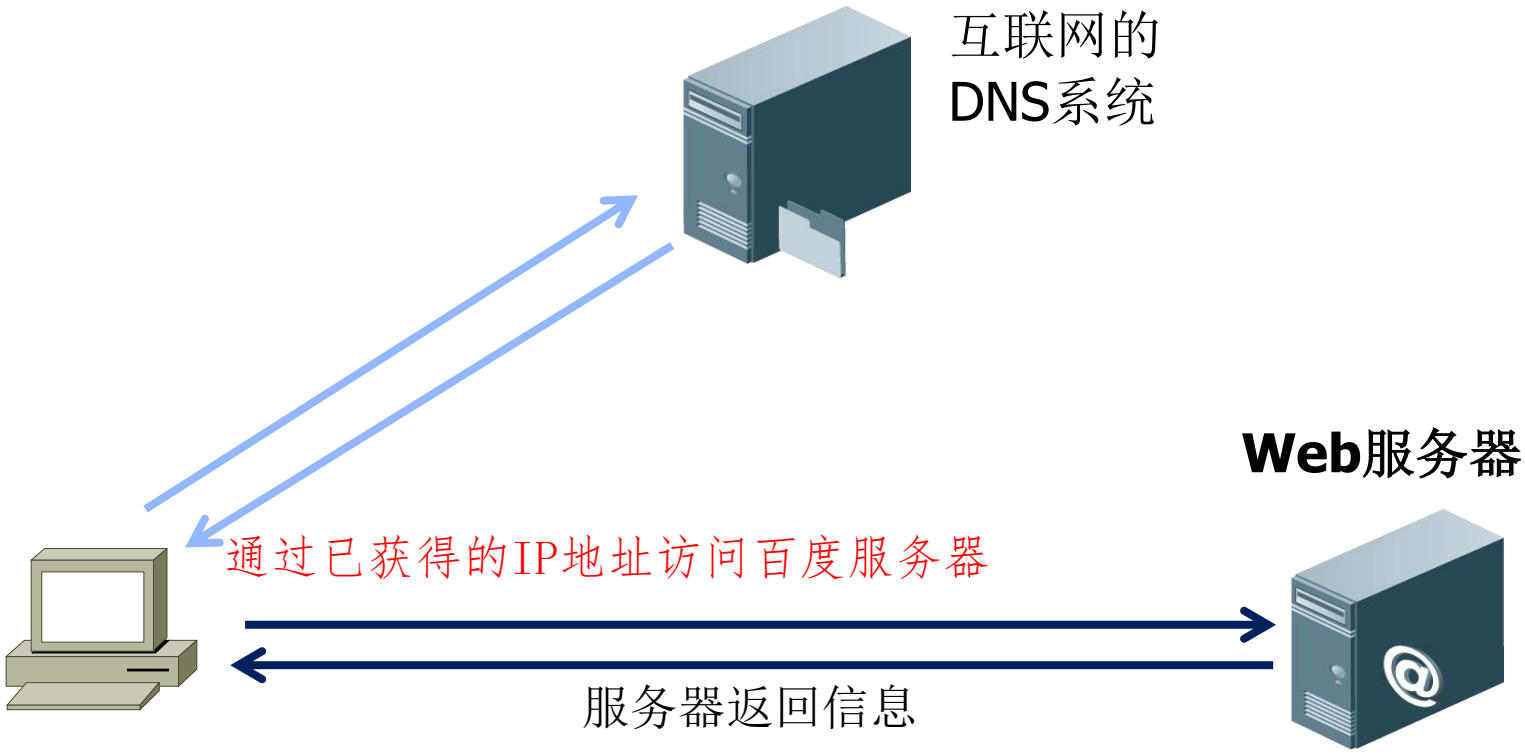


互联网的DNS系统

Web服务器

访问：www.baidu.com

现在，用户主机知道百度的IP地址了！


互联网的
DNS系统
Web服务器
通过已获得的IP地址访问百度服务器
服务器返回信息
客户端浏览器将服务器
返回的信息组织成网页
（结束）

1.DNS概述

- DNS的基本解析过程总结
  - 当某一个应用进程需要把域名解析为IP地址时，该应用进程就调用DNS解析程序，并向DNS服务器发出解析请求（该进程就成为DNS的一个客户），把待解析的域名放在DNS请求报文中，并以UDP用户数据报文方式发给域名服务器。（使用UDP减少开销）
  - 域名服务器在查找域名后，把对应的IP地址放在回答报文中返回。
  - 应用进程获得目的主机的IP地址后即可进行通信。

1.DNS概述

- 互联网域名注册服务机构


首页
产品中心
商城
服务与支持
合作伙伴
亲，请登录 | 免费注册 | 用户中心 | 购物车(0) | 管理控制台
DNSPOD
输入您想注册的域名，例如: dnspod
.com
查询域名
.com 55元 .net 55元 .xyz 11元 .cn 25元 | 域名价格总览 | 批量查询
域名首购用户专享
域名礼包买1送3 首购用户领券再减10元
域名续费
便宜到底，操作简单
域名转入
一键转入，管理方便
域名解析
无限域名，实时生效
D+
精准接入，稳定可靠


xuchenggang
.com
查 询
多选模式
中资源
www.zzy.cn
英文域名
中文域名
域名查询结果
哪些新顶级域名后缀支持备案?
xuchenggang.com (已被注册)
详细 访问
xuchenggang.wang (尚未注册)
音同“网”，符合国人认知
¥22元/首年
立即注册
xuchenggang.top (尚未注册)
代表着事物最美好的状态
¥9元/首年
立即注册
xuchenggang.net.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.com.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.net (尚未注册)
国际通用顶级域名
¥50元/首年
立即注册
xuchenggang.org.cn (尚未注册)
中国国家顶级域名
¥30元/首年
立即注册
xuchenggang.info (尚未注册)
网络信息服务的首选域名
¥150元/首年
立即注册
xuchenggang.cc (尚未注册)
可理解为Commercial Company，即商业公司
¥300元/首年
立即注册
xuchenggang.biz (尚未注册)
business的缩写，代表着商业领域
¥28元/首年
立即注册
xuchenggang.org (尚未注册)
社会组织机构首选域名
¥80元/首年
立即注册

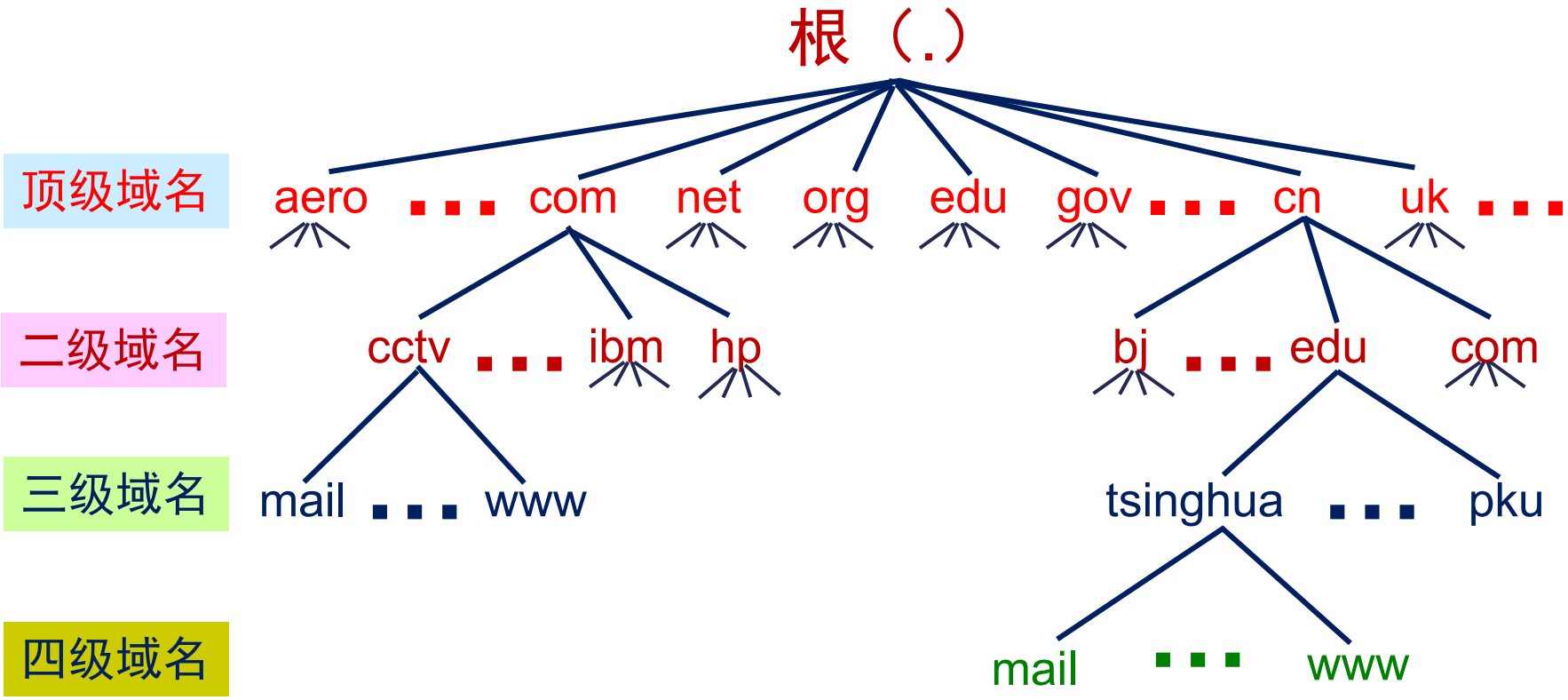
1.DNS概述

树状层次结构

- 域名采用了树状层次结构的命名方式。
- 所有的域名都以英文的“ . ”开始，是域名的根；
- 根的下面是顶级域名，
- 顶级域名下面还可以有下一级域名，例如二级、三级、四级…….
- 各级域名之间用**点**隔开

… . 三级域名 . 二级域名 . 顶级域名

互联网的域名空间


根（.）
顶级域名
二级域名
三级域名
四级域名
aero
com
net
org
edu
gov
cn
uk
cctv
ibm
hp
bj
edu
com
mail
www
tsinghua
pku
mail
www

1.DNS概述

主机名

- 企业或个人申请了域名后，可以根据自身需要在该域名下添加主机名，也可以根据需要创建子域名。
- 主机名表示是该域中的某个主机（通常是服务器）的名字；
- 例如：
  - 河南中医药大学申请的域名是　　．hactcm.edu.cn

举例：根据工作需要，河南中医药大学设置了一台Web服务器和一台邮件服务器

mail 是主机名

http://mail.hactcm.edu.cn

www 是主机名

http://www.hactcm.edu.cn

1.DNS概述

完全限定域名（FQDN）

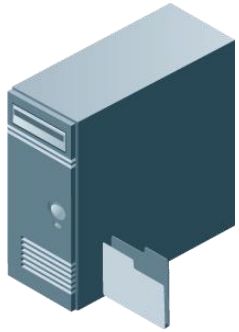
- 域名是全球唯一的，“主机名+域名”肯定也是全球唯一的。
- “主机名+域名”称为完全限定域名，即FQDN。
- FQDN是Fully Qualified Domain Name的缩写，含义是完整的域名。
- 例如：　www.hactcm.edu.cn
- 我们通常所说的网站的网址，严格来说是完全限定域名。

1.DNS概述

域名和物理服务器是一 一对应吗？

- 主机名和物理服务器并不一定是一一对应关系，例如，

network.xg.hactcm.edu.cn
database.xg.hactcm.edu.cn
csharp.xg.hactcm.edu.cn
computer.xg.hactcm.edu.cn

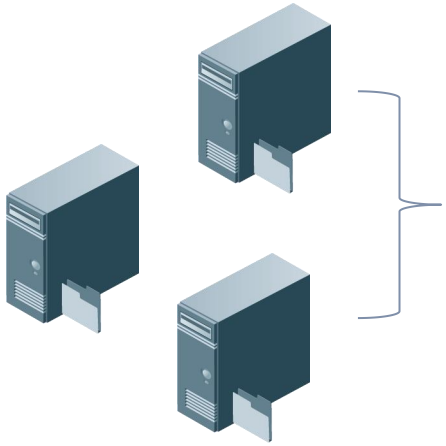


多主机名 → 1台物理服务器

1.DNS概述

域名和物理服务器是一 一对应吗？

- 对于访问量特别大的网站，会把业务（例如Web服务）镜像到多台服务器上，并具有不同的IP地址。这样就可以使不同的客户访问不同的服务器，达到负载均衡的目的。



多台服务器 → 同一主机名（域名）

www.baidu.com

1.DNS概述

总结

- 用户在访问互联网上的服务（器）时，通常使用对方的域名进行访问，而不是直接使用不易记忆的IP地址；
- 互联网网上的域名是需要申请、审批的，从而保证其唯一性；
- 域名是有其特殊格式的，从右向左，依次是根域名、顶级域名、二级域名、三级域名……，中间用“.”隔开。

二、域名服务器

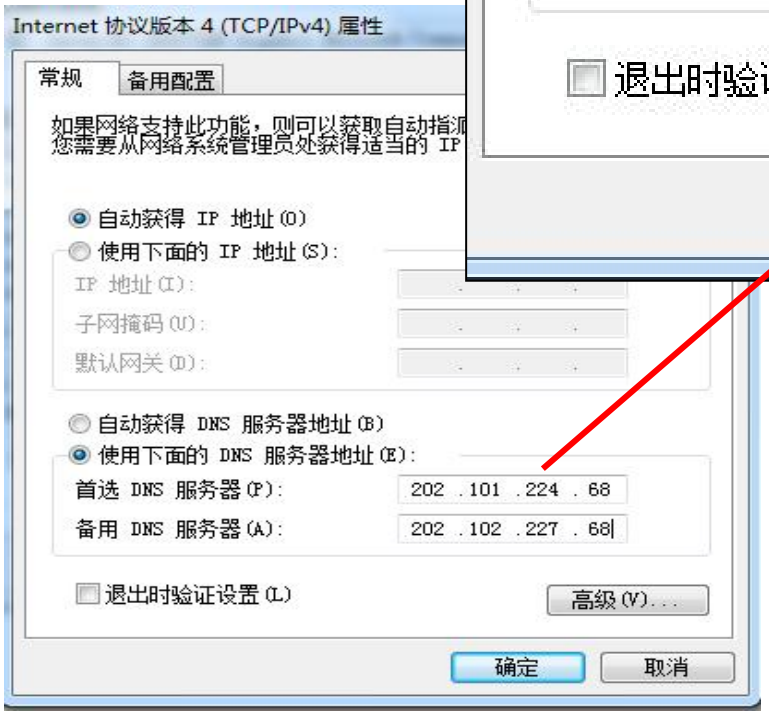
2. 域名服务器

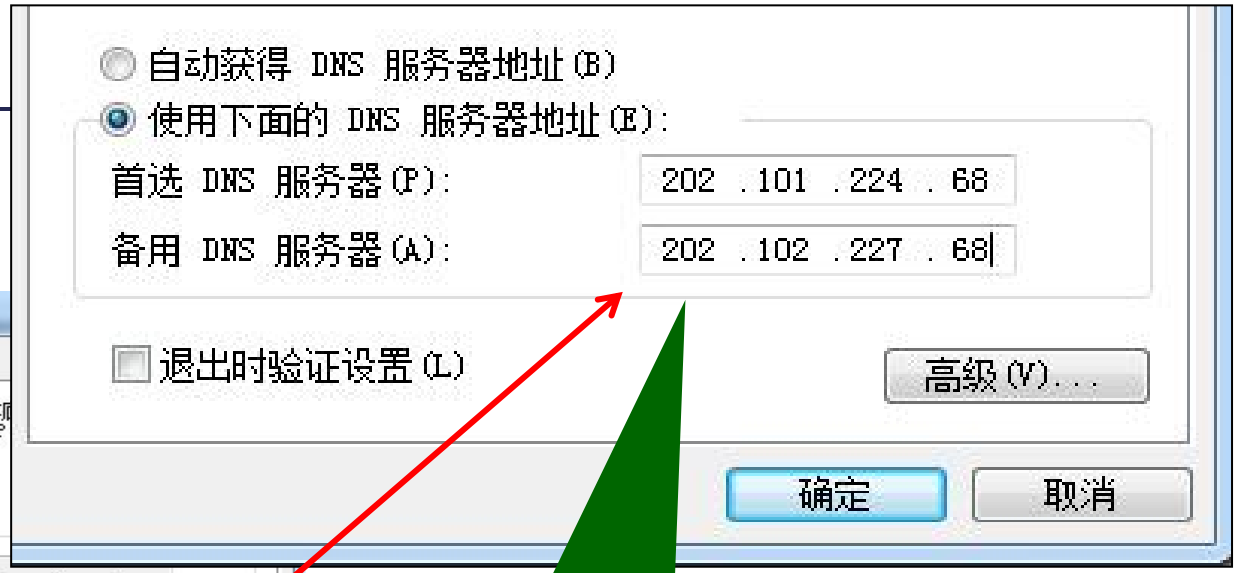
2.1 域名服务器的基本作用

2. 域名服务器

- 域名服务器的作用（简化描述）
  - 可以把互联网上的“域名——IP地址”的对应关系看成是一个数据库；
  - 假设把这个“数据库”放入一台计算机，这台计算机通过域名解析程序，专门向互联网上的用户提供“域名——IP地址”的解析和查询服务，被称作“域名服务器”；
  - 思考：
    - 互联网用户要想使用域名服务，就必须事先知道域名服务器的IP地址；
    - 配置举例

客户机的配置

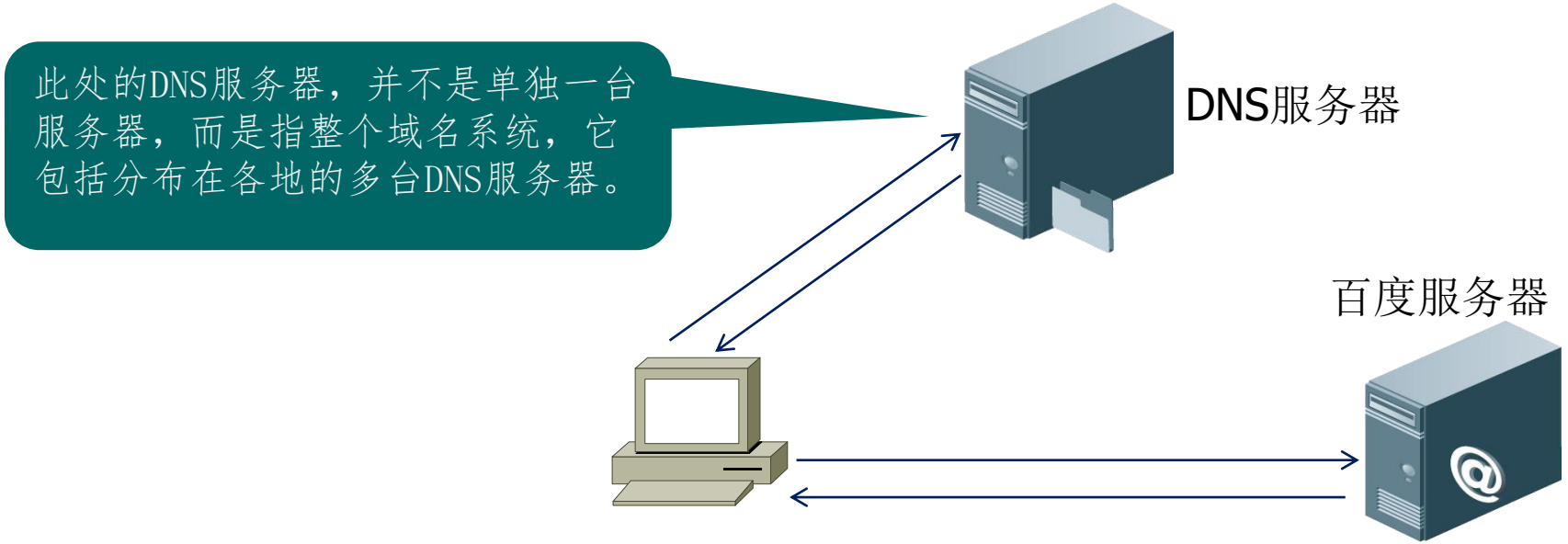




客户机事先要知道DNS服务器的IP地址

2. 域名服务器

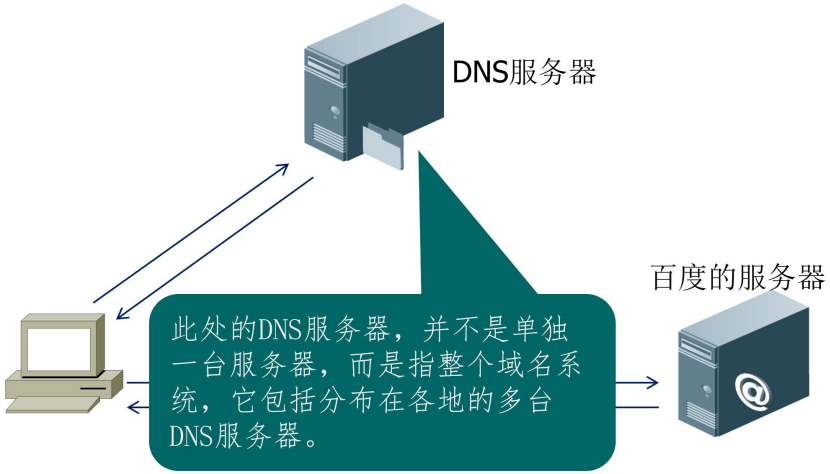
- 引申分析：能让一台DNS服务器负责全球域名的解析吗？
  - 全球的域名解析需要一个健壮的、可扩展的域名解析体系架构，即要把域名解析的任务分摊到多个DNS服务器上。



对域名系统（DNS）的进一步认识

- 前面提到：“互联网用户要想使用域名服务，就必须事先知道域名服务器的IP地址”

问题：互联网上的域名系统中，有非常多的域名服务器，我需要事先知道哪一个的IP地址？



2.2 域名服务器的分类

2. 域名服务器

- 域名服务器的分类
  - 根据域名服务器所起的作用，可以把域名服务器划分为以下四种不同的类型：

根域名服务器
顶级域名服务器
权限域名服务器

本地域名服务器

2. 域名服务器

- 整个域名系统的服务，是通过分布在各地的域名服务器来实现的。
- 互联网上的DNS域名服务器是按照层次和区域安排的；每一个域名服务器都只对整个域名体系中的一部分进行管辖；
  - 一个DNS服务器所负责管辖的范围叫做区。一个区内设置的DNS服务器通常叫做权限域名服务器，用来保存该区中所有主机的域名到IP地址的映射（即域名记录）。

例：河南中医药大学有很多网站，对应的有IP地址

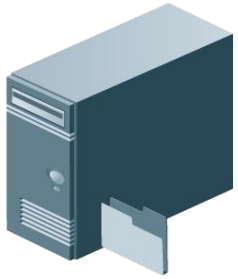
www.hactcm.edu.cn	211.69.33.10
mail.hactcm.edu.cn	211.69.33.20
ftp.hactcm.edu.cn	211.69.47.10
xg.hactcm.edu.cn	211.69.47.20
……	……

这种映射关系，由中医药大学内部的一台DNS服务器（假设其IP地址是211.69.32.8）负责解析

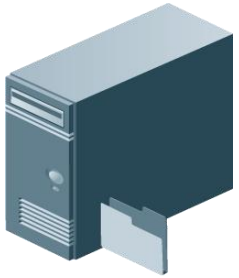
2. 域名服务器

- 我们可以“告诉”自己的PC：若想访问www.hactcm.edu.cn，就去找DNS服务器211.69.32.8行解析。
- 问题：
  1. 若我想访问www.baidu.com，该找谁来解析？
  2. 若北京的一台PC想访问www.hactcm.edu.cn，他怎么知道该找211.69.32.8来解析？

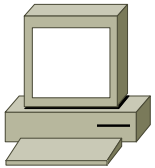
DNS_b



DNS_c

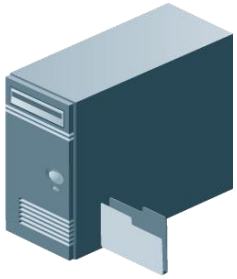


域名解析请求到底发给谁？

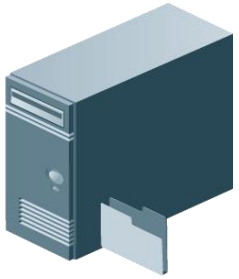


用户主机

DNS_a

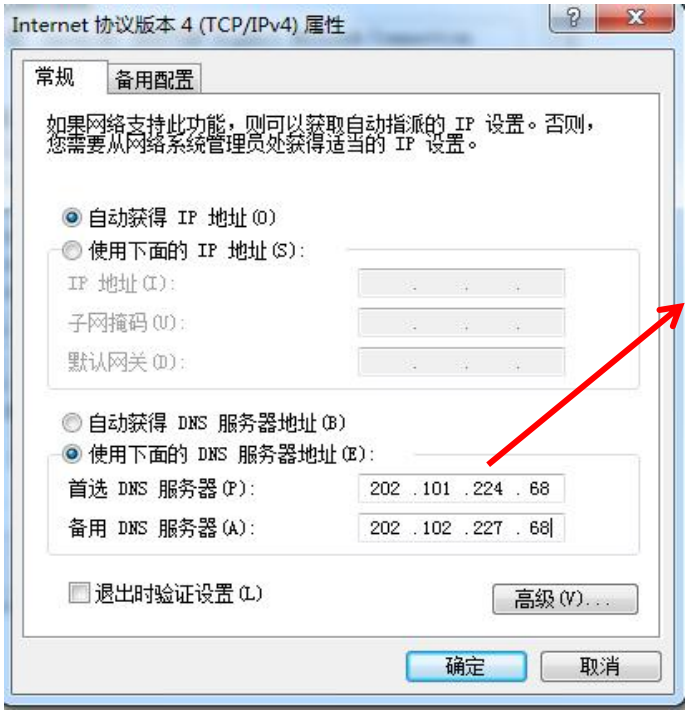


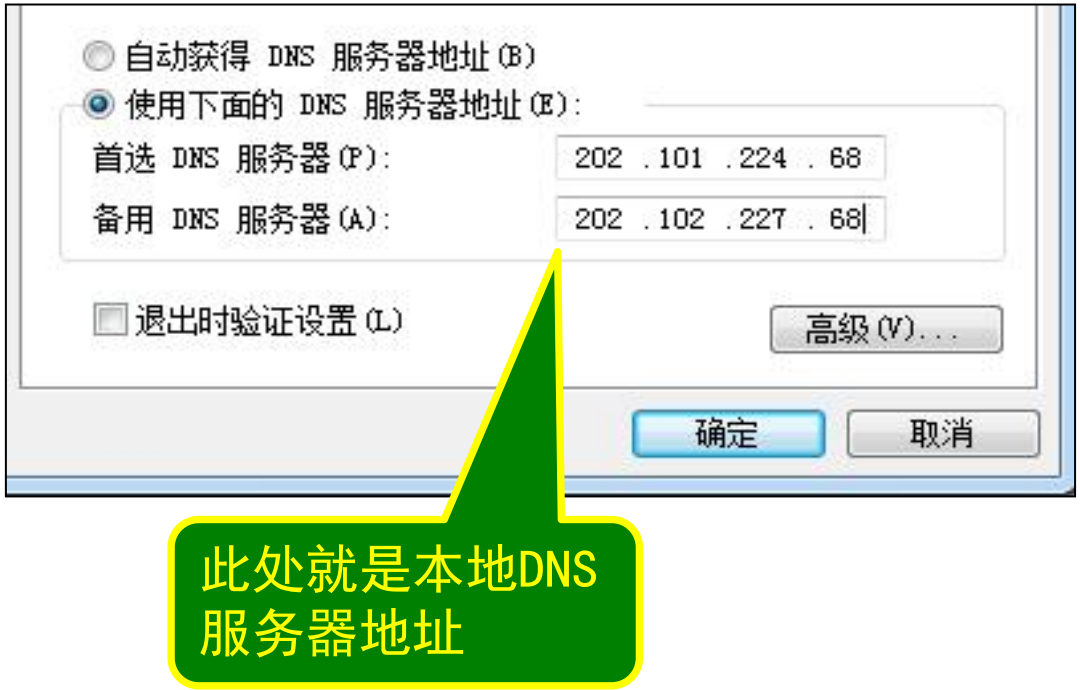
DNS_d



2. 域名服务器

- 本地域名服务器
  - 用户在系统中所设置的首选DNS服务器，就被认为是本地域名服务器；





2. 域名服务器

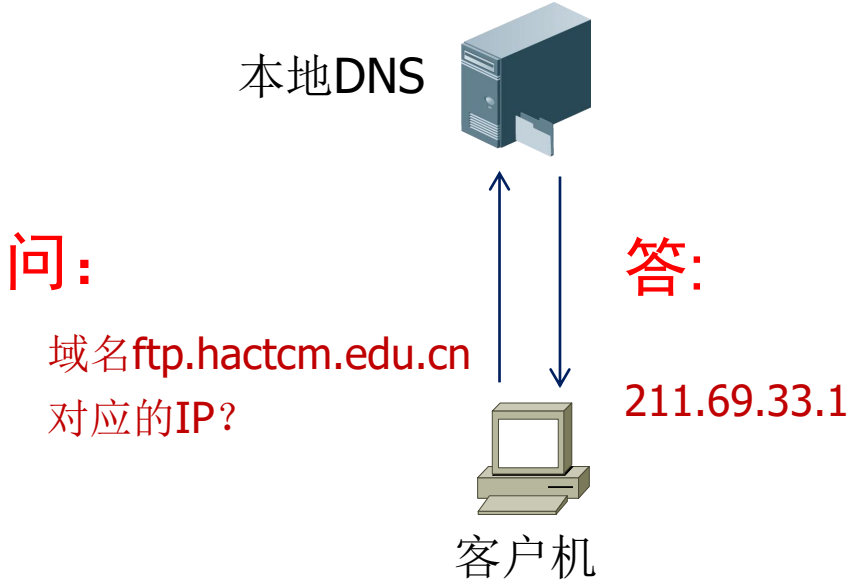
- 本地域名服务器
  - 当客户机发出 DNS 请求时，这个请求报文就首先发送给本地域名服务器。
  - 每一个互联网服务提供者 ISP，或一个大学，甚至一个大学里的系，都可以提供一个域名服务器，用作本区域客户机的本地域名服务器；
  - 本地域名服务器在域名解析过程中起着重要作用，帮助客户机从互联网的域名系统中获得域名解析结果，并将结果发回给客户机。

2. 域名服务器

- 本地域名服务器
  - 举例：
  - 河南中医药大学校园网内部有一台DNS服务器（假设其IP地址是211.69.32.8），该服务器内部记录有河南中医药大学内部各应用服务器（例如ftp、Web、mail等服务器）的主机名和IP地址的映射关系；
  - 校园网用户可以把该服务器作为自己的本地DNS服务器，通过该服务器来进行域名解析，例如访问ftp.hactcm.edu.cn，通过该DNS服务器可解析出其对应的IP地址。

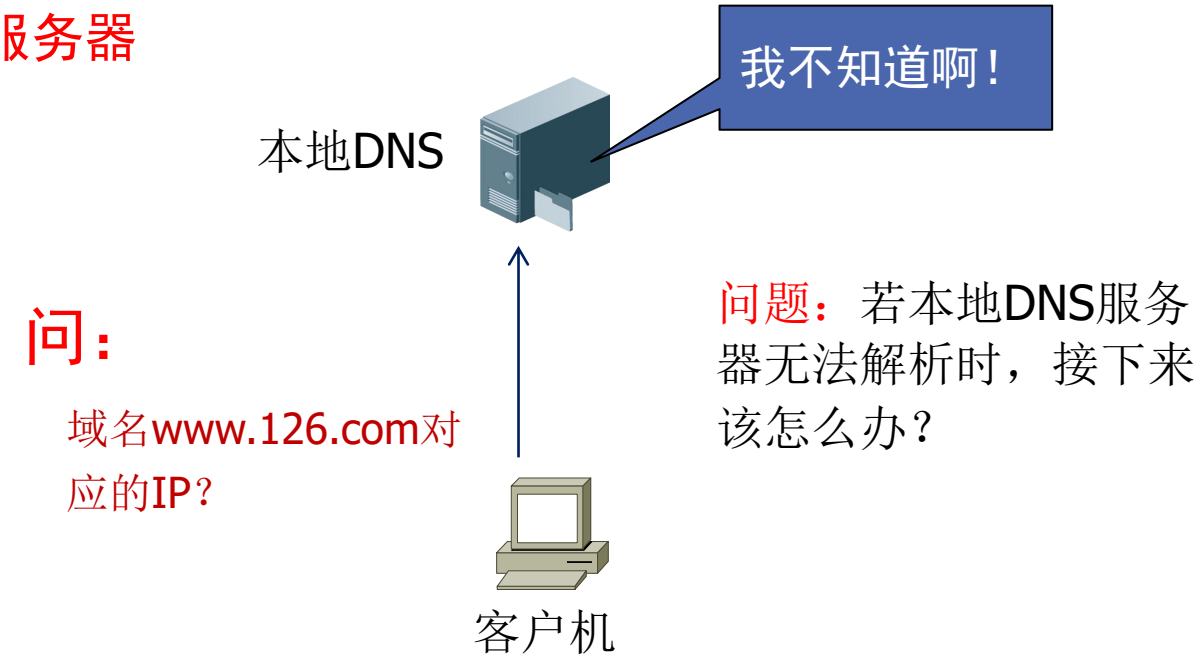
2. 域名服务器

- 本地域名服务器



2. 域名服务器

- 本地域名服务器



2. 域名服务器

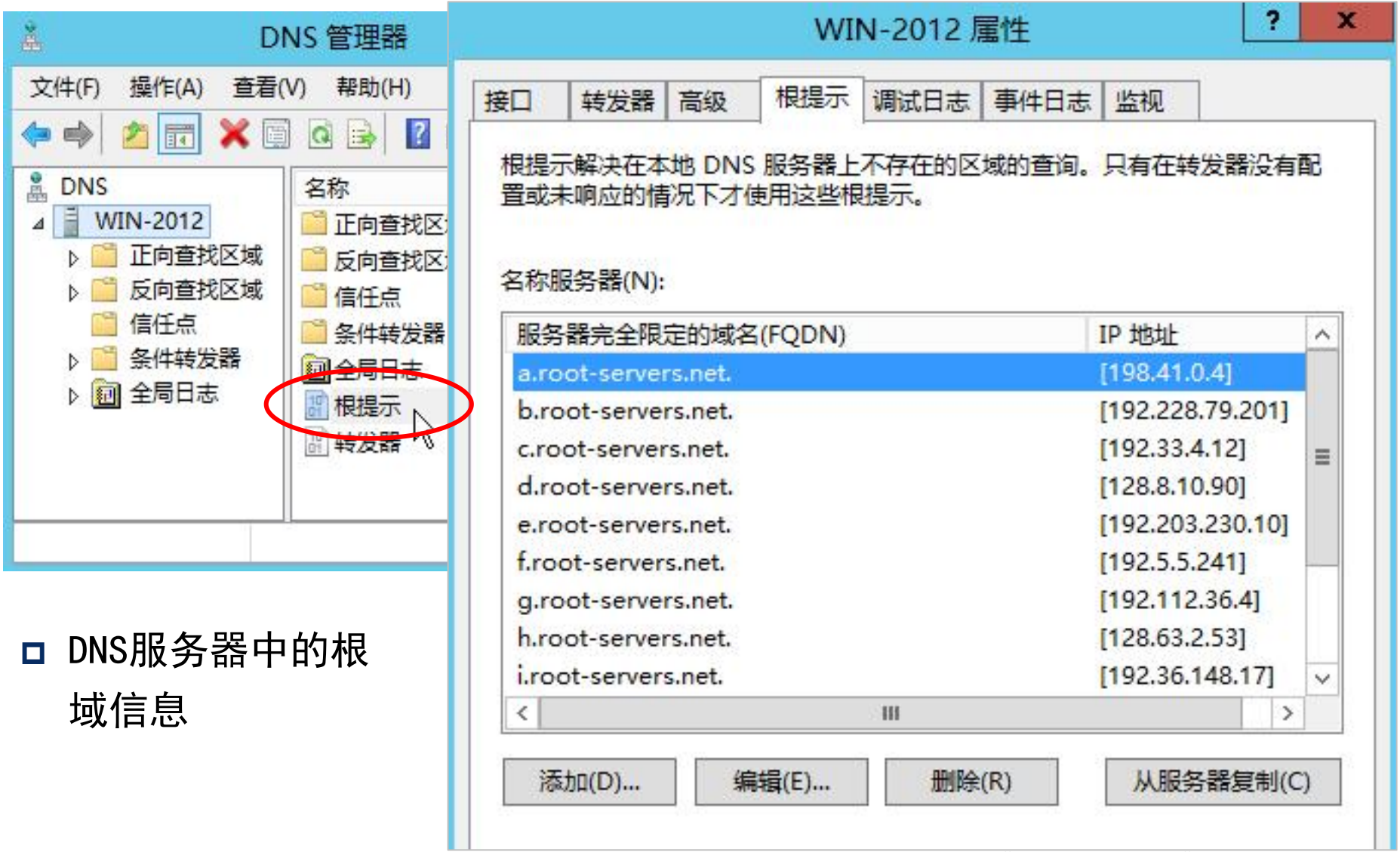
- 根域名服务器
  - 在给一台服务器安装DNS服务程序时，会自动安装13套根域名服务器的相关信息，包括每台根域名服务器的域名和对应的IP地址。因此，当本地DNS服务器不知道待查域名的IP地址时，就把请求发给根域服务器；
  - 根DNS服务器是由互联网管理机构配置建立的，是最高层次的DNS服务器，负责对互联网上所有顶级DNS服务器进行管理，含有全部顶级DNS服务器的IP地址和域名映射。
  - 根DNS服务器并不直接用于域名解析，仅负责管理顶级DNS服务器的相关记录。当本地DNS服务器解析不了某个域名时，告诉本地DNS服务器去找哪个顶级DNS服务器。【我不知道目的地在哪？但我知道下一步怎么走！】

2. 域名服务器

- 根域名服务器
  - 在互联网上共有13 套不同 IP 地址的根域名服务器，它们的名字是用一个英文字母命名，从a 一直到 m（前13 个字母）。相应的域名分别是：

    a.rootservers.net
    b.rootservers.net
    ……
    m.rootservers.net

  - 到 2021 年，全球共有1375个根域名服务器在运行。这样做的目的是为了方便用户，使世界上大部分 DNS 域名服务器都能就近找到一个根域名服务器



- DNS服务器中的根域信息

2. 域名服务器

- 全球

表 5-02 13 台主根 DNS 服务器的管理机构和 IP 地址

名称	管理单位及设置地点	IP 地址
A	INTERNIC.NET（美国，弗吉尼亚州）	198.41.0.4
B	美国信息科学研究所（美国，加利弗尼亚州）	128.9.0.107
C	PSINet 公司（美国，弗吉尼亚州）	192.33.4.12
D	马里兰大学（美国马里兰州）	128.8.10.90
E	美国航空航天管理局（美国加利弗尼亚州）	192.203.230.10
F	因特网软件联盟（美国加利弗尼亚州）	192.5.5.241
G	美国国防部网络信息中心（美国弗吉尼亚州）	192.112.36.4
H	美国陆军研究所（美国马里兰州）	128.63.2.53
I	Autonomica 公司（瑞典，斯德哥尔摩）	192.36.148.17
J	VeriSign 公司（美国，弗吉尼亚州）	192.58.128.30
K	RIPE NCC（英国，伦敦）	193.0.14.129
L	IANA（美国，弗吉尼亚州）	198.32.64.12
M	WIDE Project（日本，东京）	202.12.27.33

2. 域名服务器

- 顶级域名服务器
  - 负责管理在该顶级域名服务器注册的所有二级域名。
  - 当收到 DNS 查询请求时，就给出相应的回答，可能是最后的结果，也可能是下一步应当找的域名服务器（权限域名服务器）的 IP 地址。

2. 域名服务器

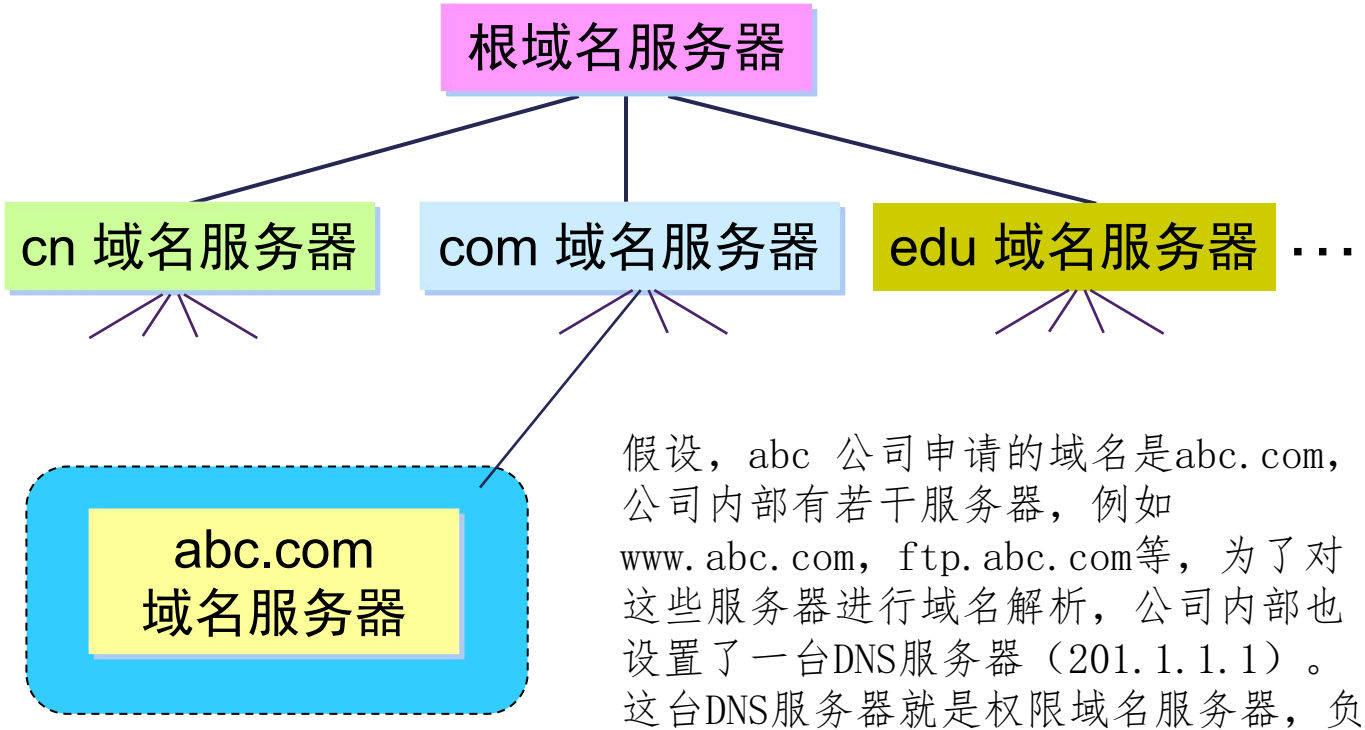
- 权限域名服务器（又被称为权威域名服务器）
  - 这就是前面已经讲过的负责一个区域的域名服务器。
  - 当一个权限域名服务器还不能给出最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权限域名服务器。
  - 例如 211.69.32.8　就是河南中医药大学的 权限域名服务器，它由河南中医药大学负责建设维护，负责河南中医药大学内部的服务器的域名解析，该DNS服务器在其上级域中有备案。

➢ 树状结构的 DNS 域名服务器

根域名服务器

顶级域名服务器

权限域名服务器



假设，abc 公司申请的域名是abc.com，公司内部有若干服务器，例如www.abc.com，ftp.abc.com等，为了对这些服务器进行域名解析，公司内部也设置了一台DNS服务器（201.1.1.1）。这台DNS服务器就是权限域名服务器，负责对本公司内部的服务器域名进行解析

三、域名解析的过程

举例：

一台客户机想访问www. 126. com

首先，客户机先在本机上查找关于www.126.com的记录

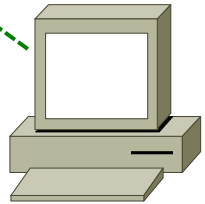
第1步：

客户机所做的的工作

www.126.com

IP地址?

访问：www.126.com



（1）步骤1：查询自己的缓存，看看有没有记录www.126.com对应的IP地址，若有直接获得。

否

（2）步骤2：查询自己的hosts文件，看看有没有记录www.126.com对应的IP地址，若有直接获得。

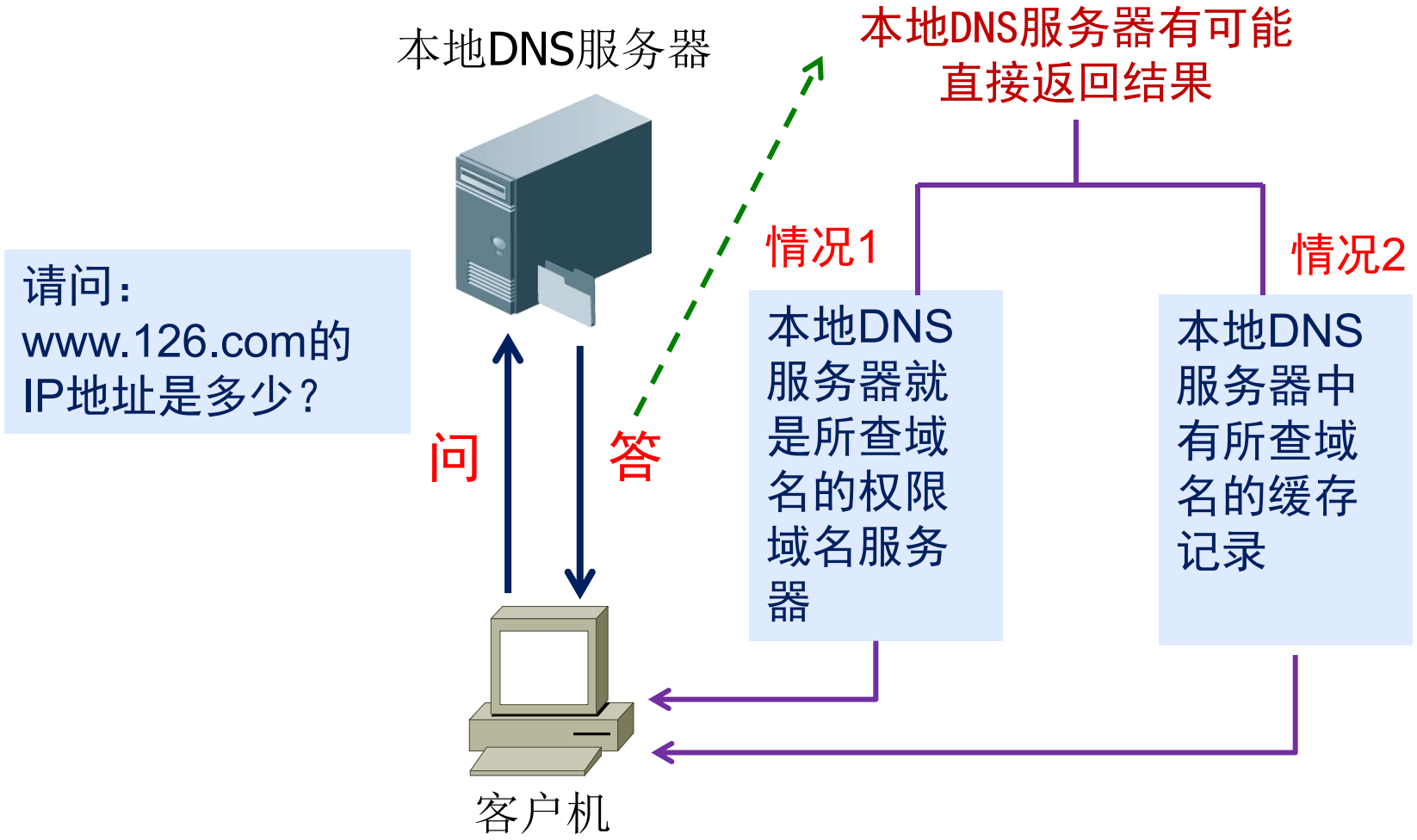
否

（3）步骤3：向本地DNS服务器发出域名解析请求。

域名解析过程举例

若本机上没有关于www.126.com的记录，则客户机把DNS解析请求发给本地DNS服务器

假设： 本地DNS服务器是 211.69.32.8


本地DNS服务器
本地DNS服务器有可能
直接返回结果
请问：
www.126.com的
IP地址是多少？
问
答
情况1
本地DNS
服务器就
是所查域
名的权限
域名服务
器
情况2
本地DNS
服务器中
有所查域
名的缓存
记录
客户机

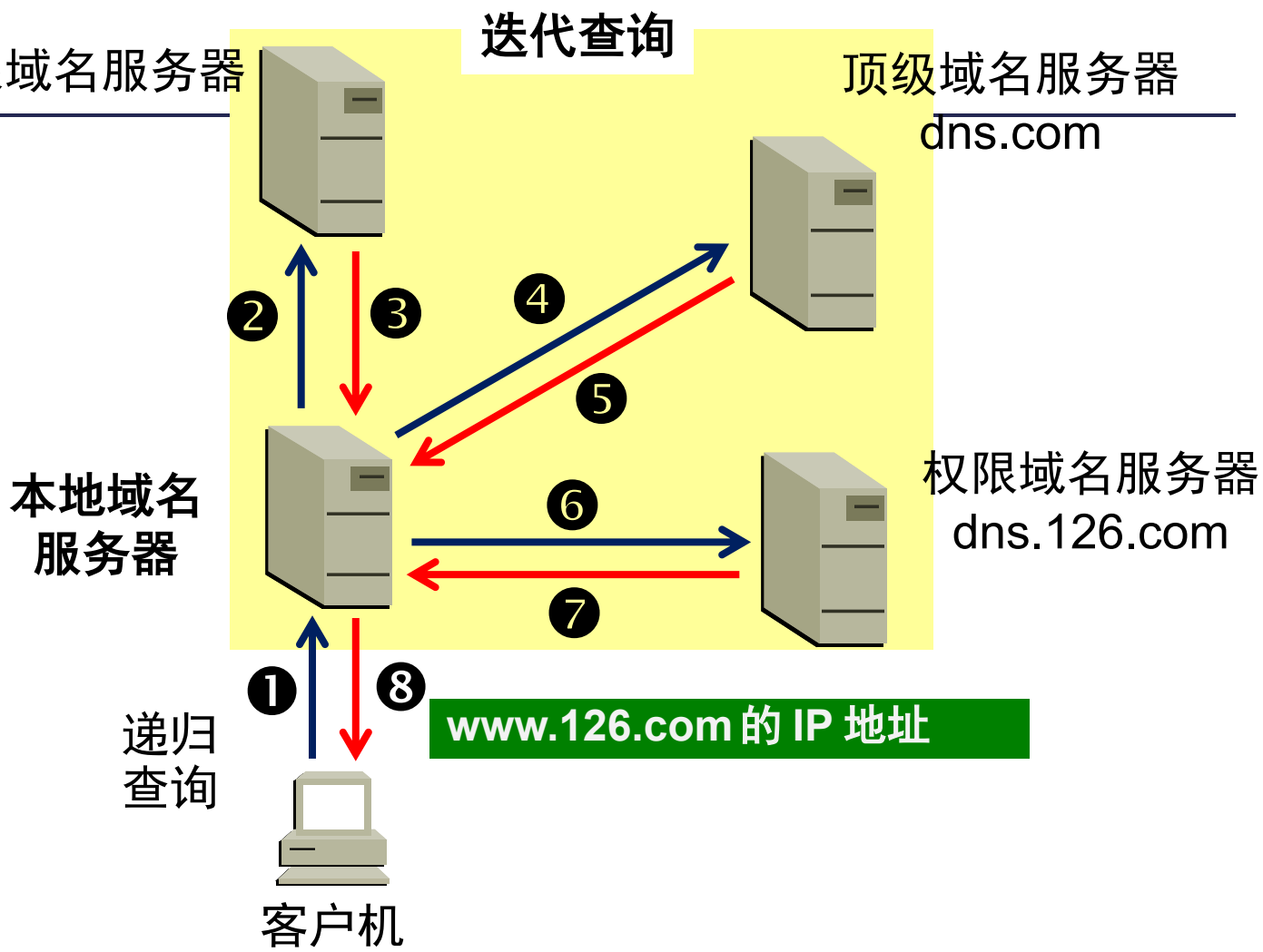
域名解析过程举例

如果本地DNS服务器不能解决问题，怎么办？

如果本地DNS服务器无法解析域名 www.126.com，则本地DNS服务器就向互联网上的域名系统发出解析请求。

具体步骤如下：

本地域名服务器采用迭代查询



域名的解析过程

- 主机向本地域名服务器的查询一般都是采用递归查询。如果本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向根域名服务器继续发出查询请求报文。
- 本地域名服务器向根域名服务器的查询通常是采用迭代查询。当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。
- 以此类推，直至结束。

例2：一个电信用户访问 www. hactcm.edu.cn

举例：一个电信用户访问 www. hactcm.edu.cn

1. 用户主机提出域名解析请求，并将该请求发给本地DNS服务器（电信的公共DNS）。
2. 本地DNS服务器收到请求后就去查询自己的缓存，如果有该条记录，则会将查询的结果返回给客户端。
3. 本地DNS服务器无法解析该域名，因此，本地域名服务器就以 DNS 客户的身份向根DNS（13台根DNS服务器的IP信息默认均存储在DNS服务器中，当需要时就会去有选择性的连接）发出解析请求。

举例：一个电信用户访问 www. hactcm.edu.cn

4. 根DNS服务器收到请求后，也不知道该域名的IP地址，但是，它判断这个域名的顶级域名是cn，根DNS服务器就会把. cn的顶级域名DNS服务器的IP地址返回给本地DNS服务器。
5. 本地DNS服务器收到这个地址后，就开始联系dns. cn，并将此请求发给他。该顶级域名服务器经过解析，把dns. edu. cn的地址返回给本地域名服务器。

- 含义：我虽然不知道www. hactcm. edu. cn的IP，但我知道该域名是属于edu. cn域的，而我知道dns. edu. cn这台域名解析服务器的IP，你去找它问问吧。

举例：一个电信用户访问 www. hactcm.edu.cn

6. 本地DNS服务器收到dns. edu. cn域名服务器的地址后，就会重复上面的动作。
7. dns. edu. cn收到请求后，进行解析。它也不知道www. hactcm. edu. cn的IP，但它知道该域名属于. hactcm. edu. cn这个域，而它知道dns. hactcm. edu. cn这个权限域名服务器的地址，因此它把该地址返回给本地DNS。

- 注意：此处的dns. hactcm. edu. cn就是一个权限域名服务器。

举例：一个电信用户访问 www. hactcm.edu.cn

8. 本地DNS服务器收到这个权限域名服务器地址后，再次重复上面的动作，找到dns.hactcm.edu.cn这台权限域名服务器，并把域名解析请求发给它；
9. 该DNS服务器在自己的数据库中查到了www.hactcm.edu.cn这个域名所对应的IP，并把地址返回给本地DNS服务器。

准确的讲：　www.hactcm.edu.cn —— 211.69.32.5　是权限域名服务器（dns.hactcm.edu.cn）的数据库当中的一条记录（A记录）。

至此，域名系统的解析工作完成了。

举例：一个电信用户访问 www. hactcm.edu.cn

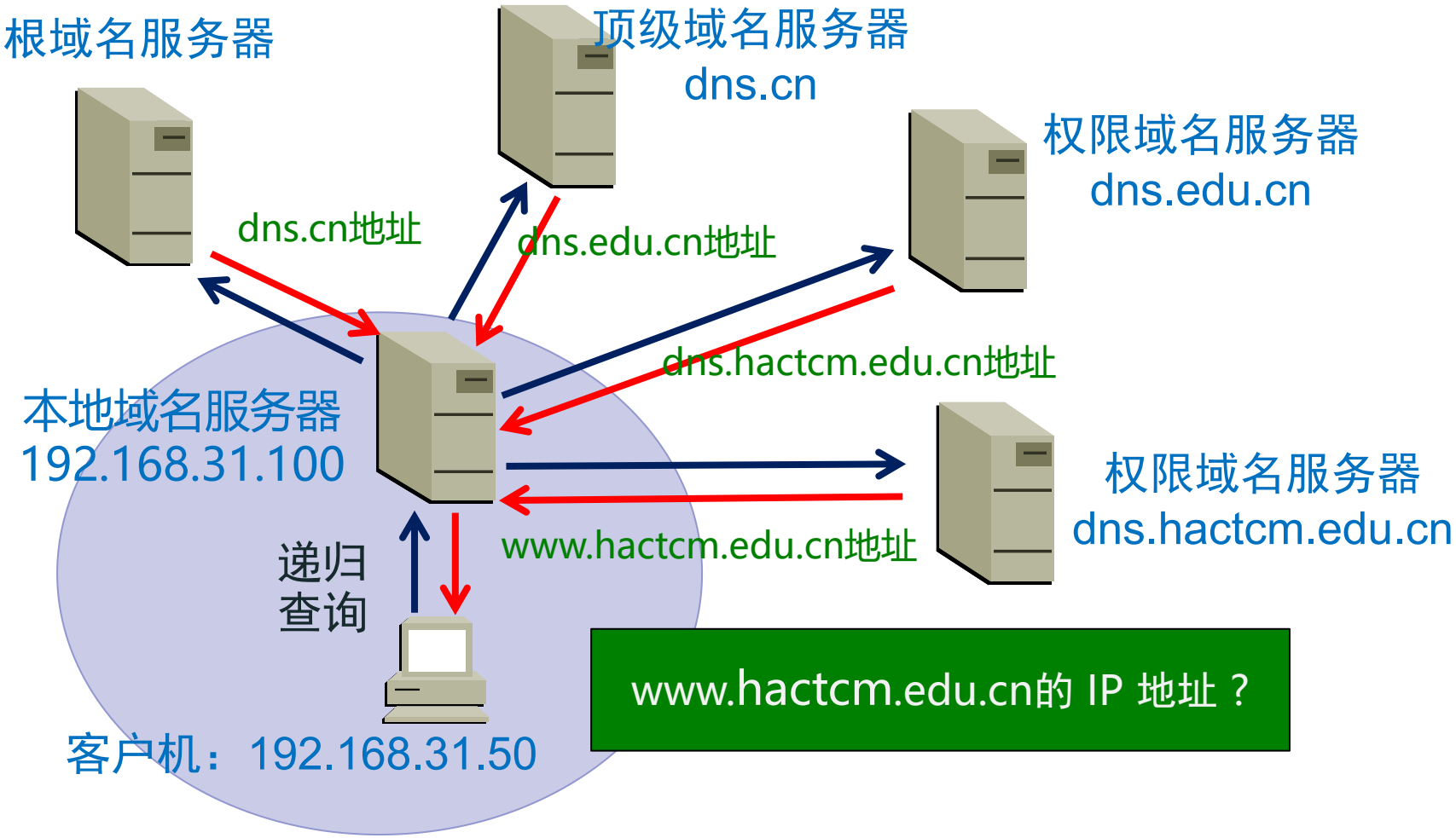
- 现在，本地DNS服务器终于获得www.hactcm.edu.cn的IP，然后把这个IP返回给客户机，整个解析工作全部完成。接下来，客户端主机（该电信用户）根据此IP去访问www.hactcm.edu.cn。
- 提醒：
  - 可以看出，在整个解析过程中，客户端主机把域名解析请求发给本地域名服务器以后，就一直处理等待状态，他不需要做任何事，也做不了什么。
  - 本地域名服务器收到该请求，就代替客户端主机向因特网的域名解析系统发出查询请求。直到把结果返回给客户端主机。（注意：查询析结果可能失败）

例3：抓包分析域名解析过程

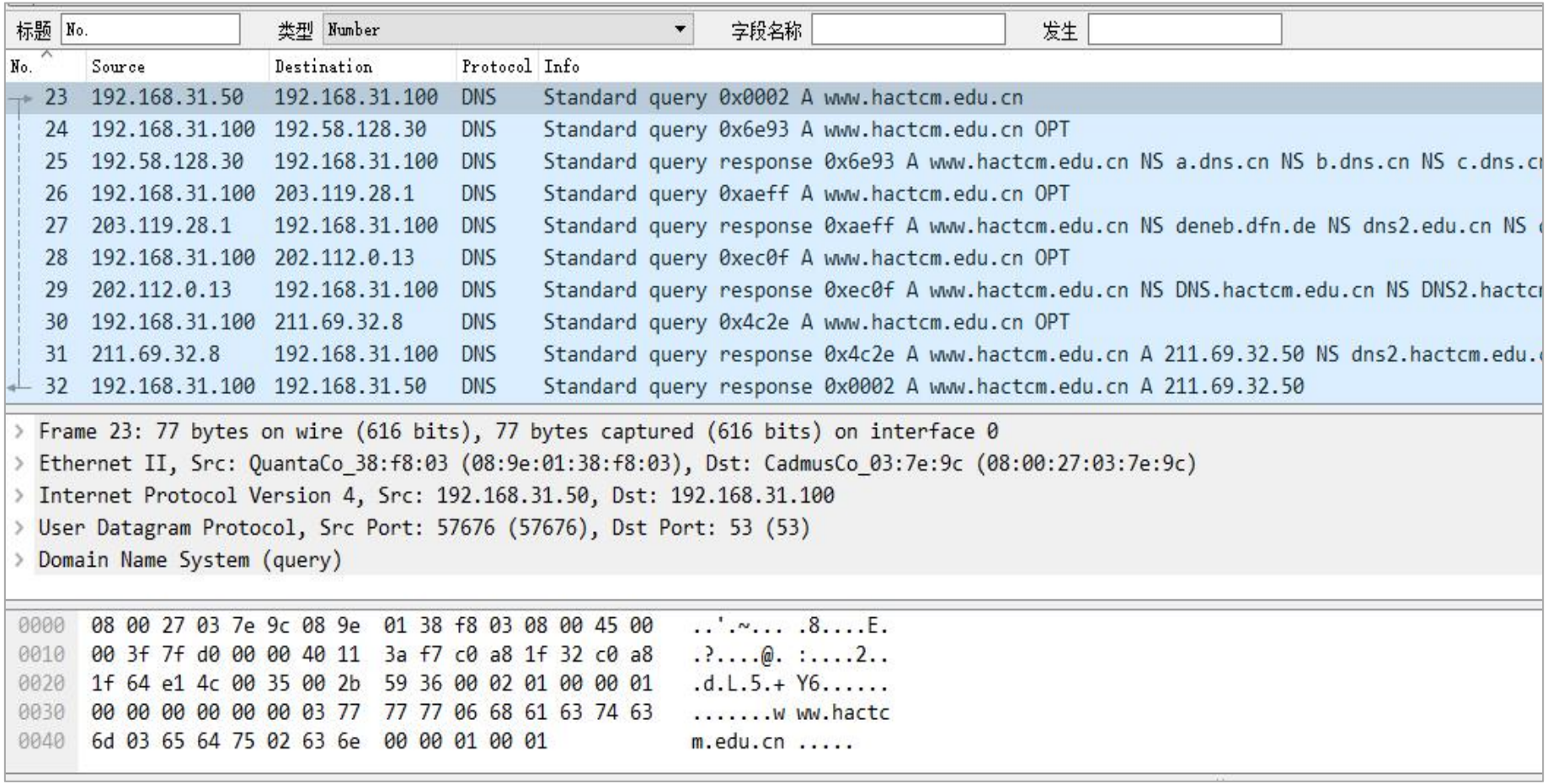
【案例】抓包分析域名解析过程

- 场景描述
  - 用户在家中上网，通过无线路由器NAT接入互联网（ISP是河南电信）
  - 用户主机IP：192.168.31.50，本地DNS是192.168.31.100
  - 用户现在访问www.hactcm.edu.cn，即部署在河南中医药大学的一台WWW服务器
  - 域名.hactcm.edu.cn对应的权限DNS地址是211.69.32.8，该域名及对应的权限DNS服务器已经在中国教科网（ISP）中进行了注册；
  - 假设，本地DNS中（包括缓存中），没有www.hactcm.edu.cn对应的域名记录信息。

➢ 域名解析过程总体描述


根域名服务器
顶级域名服务器
dns.cn
权限域名服务器
dns.edu.cn
dns.cn地址
dns.edu.cn地址
dns.hactcm.edu.cn地址
本地域名服务器
192.168.31.100
递归
查询
www.hactcm.edu.cn地址
权限域名服务器
dns.hactcm.edu.cn
www.hactcm.edu.cn的 IP 地址？
客户机：192.168.31.50

➢ 域名解析过程的整体报文一览

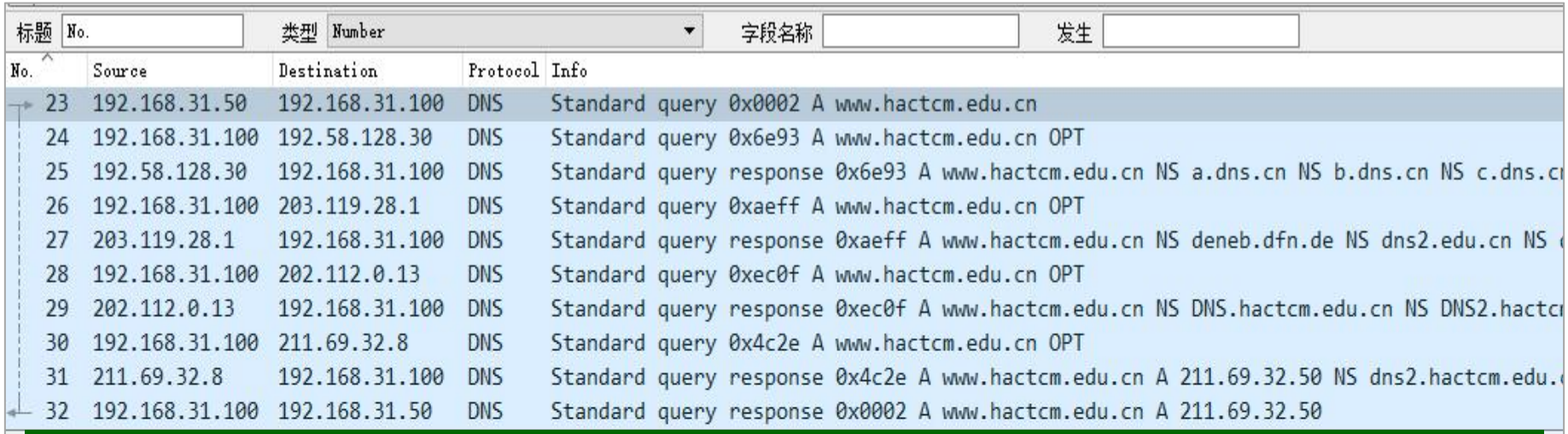


标题 No. 类型 Number 字段名称 发生

No.	Source	Destination	Protocol	Info
23	192.168.31.50	192.168.31.100	DNS	Standard query 0x0002 A www.hactcm.edu.cn
24	192.168.31.100	192.58.128.30	DNS	Standard query 0x6e93 A www.hactcm.edu.cn OPT
25	192.58.128.30	192.168.31.100	DNS	Standard query response 0x6e93 A www.hactcm.edu.cn NS a.dns.cn NS b.dns.cn NS c.dns.cn
26	192.168.31.100	203.119.28.1	DNS	Standard query 0xaeff A www.hactcm.edu.cn OPT
27	203.119.28.1	192.168.31.100	DNS	Standard query response 0xaeff A www.hactcm.edu.cn NS deneb.dfn.de NS dns2.edu.cn NS
28	192.168.31.100	202.112.0.13	DNS	Standard query 0xec0f A www.hactcm.edu.cn OPT
29	202.112.0.13	192.168.31.100	DNS	Standard query response 0xec0f A www.hactcm.edu.cn NS DNS.hactcm.edu.cn NS DNS2.hactcm
30	192.168.31.100	211.69.32.8	DNS	Standard query 0x4c2e A www.hactcm.edu.cn OPT
31	211.69.32.8	192.168.31.100	DNS	Standard query response 0x4c2e A www.hactcm.edu.cn A 211.69.32.50 NS dns2.hactcm.edu.
32	192.168.31.100	192.168.31.50	DNS	Standard query response 0x0002 A www.hactcm.edu.cn A 211.69.32.50

```
> Frame 23: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
> Ethernet II, Src: QuantaCo_38:f8:03 (08:9e:01:38:f8:03), Dst: CadmusCo_03:7e:9c (08:00:27:03:7e:9c)
> Internet Protocol Version 4, Src: 192.168.31.50, Dst: 192.168.31.100
> User Datagram Protocol, Src Port: 57676 (57676), Dst Port: 53 (53)
> Domain Name System (query)
```

```
0000  08 00 27 03 7e 9c 08 9e  01 38 f8 03 08 00 45 00   ..'.~... .8....E.
0010  00 3f 7f d0 00 00 40 11  3a f7 c0 a8 1f 32 c0 a8   .?....@. :....2..
0020  1f 64 e1 4c 00 35 00 2b  59 36 00 02 01 00 00 01   .d.L.5.+ Y6......
0030  00 00 00 00 00 00 03 77  77 77 06 68 61 63 74 63   .......w ww.hactc
0040  6d 03 65 64 75 02 63 6e  00 00 01 00 01            m.edu.cn .....
```



(23)192.168.31.50 → 192.168.31.100 客户机 → 本地DNS

(24)192.168.31.100 → 192.58.128.30 本地DNS → 根DNS

(25)192.58.128.30 → 192.168.31.100 根DNS → 本地DNS

(26) 192.168.31.100 → 203.119.28.1 本地DNS → 顶级DNS(.cn)

(27) 203.119.28.1 → 192.168.31.100 顶级DNS(.cn) → 本地DNS

(28) 192.168.31.100 → 202.112.0.13 本地DNS → 权限DNS(.edu.cn)

(29) 202.112.0.13 → 192.168.31.100 权限DNS(.edu.cn) → 本地DNS

(30) 192.168.31.100 → 211.69.32.8 本地DNS → 权限DNS (.hactcm.edu.cn)

(31) 211.69.32.8 → 192.168.31.100 权限DNS(.hactcm.edu.cn) → 本地DNS

(32) 192.168.31.100 → 192.168.31.50 本地DNS → 客户机

(23)192.168.31.50 → 192.168.31.100 客户机 → 本地DNS

No.	Source	Destination	Protocol	Info
23	192.168.31.50	192.168.31.100	DNS	Standard query 0x0002 A www.hactcm.edu.cn

客户机向本地DNS服务器发出解析请求

客户机是192.168.31.50，本地DNS服务器是192.168.31.100

(24) 192.168.31.100 → 192.58.128.30　　本地DNS → 根DNS

No.	Source	Destination	Protocol	Info
23	192.168.31.50	192.168.31.100	DNS	Standard query 0x0002 A www.hactcm.edu.cn

No.	Source	Destination	Protocol	Info
24	192.168.31.100	192.58.128.30	DNS	Standard query 0x6e93 A www.hactcm.edu.cn OPT

本地DNS服务器（192.168.31.100）把解析请求发给一台根域名服务器，此处为192.58.128.30。

(25) 192.58.128.30 → 192.168.31.100 根DNS → 本地DNS

No.	Source	Destination	Protocol	Info
24	192.168.31.100	192.58.128.30	DNS	Standard query 0x6e93 A www.hactcm.edu.cn OPT

No.	Source	Destination	Protocol	Info
25	192.58.128.30	192.168.31.100	DNS	Standard query response 0x6e93 A www.hactcm.edu.cn

NS a.dns.cn NS b.dns.cn NS c.dns.cn NS d.dns.cn NS e.dns.cn NS…

根域名服务器（192.58.128.30）并不知道www.hactcm.edu.cn对应的IP地址是什么，不过，它发现www.hactcm.edu.cn的顶级域名是. cn，而它知道顶级域名服务器dns.cn的IP地址（203.119.28.1 ），于是，它告诉了（即应答）本地DNS服务器（192.168.31.100）

(25) 192.58.128.30 → 192.168.31.100 根DNS → 本地DNS

No.	Source	Destination	Protocol	Info
25	192.58.128.30	192.168.31.100	DNS	Standard
26	192.168.31.100	203.119.28.1	DNS	Standard
27	203.119.28.1	192.168.31.100	DNS	Standard

```
> Frame 25: 558 bytes on wire (4464 bits), 558 bytes
> Ethernet II, Src: XiaomiCo_1d:4f:3a (f0:b4:29:1d:4f
> Internet Protocol Version 4, Src: 192.58.128.30, Ds
> User Datagram Protocol, Src Port: 53 (53), Dst Port
v Domain Name System (response)
    [Request In: 24]
    [Time: 0.194208000 seconds]
    Transaction ID: 0x6e93
  > Flags: 0x8000 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 8
    Additional RRs: 9
  > Queries
  > Authoritative nameservers
  > Additional records
```

```
  Authority RRs: 8
  Additional RRs: 9
> Queries
                                                dns.cn
                                                dns.cn
                                                dns.cn
                                                dns.cn
                                                dns.cn
                                                ns.cernet.net
  > cn: type DS, class
  > cn: type RRSIG, class
v Additional records
  > a.dns.cn: type A, class IN, addr 203.119.25.1
  > b.dns.cn: type A, class IN, addr 203.119.26.1
  > c.dns.cn: type A, class IN, addr 203.119.27.1
  > d.dns.cn: type A, class IN, addr 203.119.28.1
  > e.dns.cn: type A, class IN, addr 203.119.29.1
  > ns.cernet.net: type A, class IN, addr 202.112.0.44
  > a.dns.cn: type AAAA, class IN, addr 2001:dc7::1
  > d.dns.cn: type AAAA, class IN, addr 2001:dc7:1000::1
  > <Root>: type OPT
```

根DNS反馈的.cn 域名服务器的地址 203.119.28.1

(26) 192.168.31.100 → 203.119.28.1 本地DNS → 顶级DNS .cn

No.	Source	Destination	Protocol	Info
26	192.168.31.100	203.119.28.1	DNS	Standard query 0xaeff A www.hactcm.edu.cn OPT

本地DNS服务器(192.168.31.100)向203.119.28.1发出解析请求（query）。而203.119.28.1是 .cn顶级域名服务器中的一台（即d.dns.cn）

(27) 203.119.28.1 → 192.168.31.100 顶级DNS .cn → 本地DNS

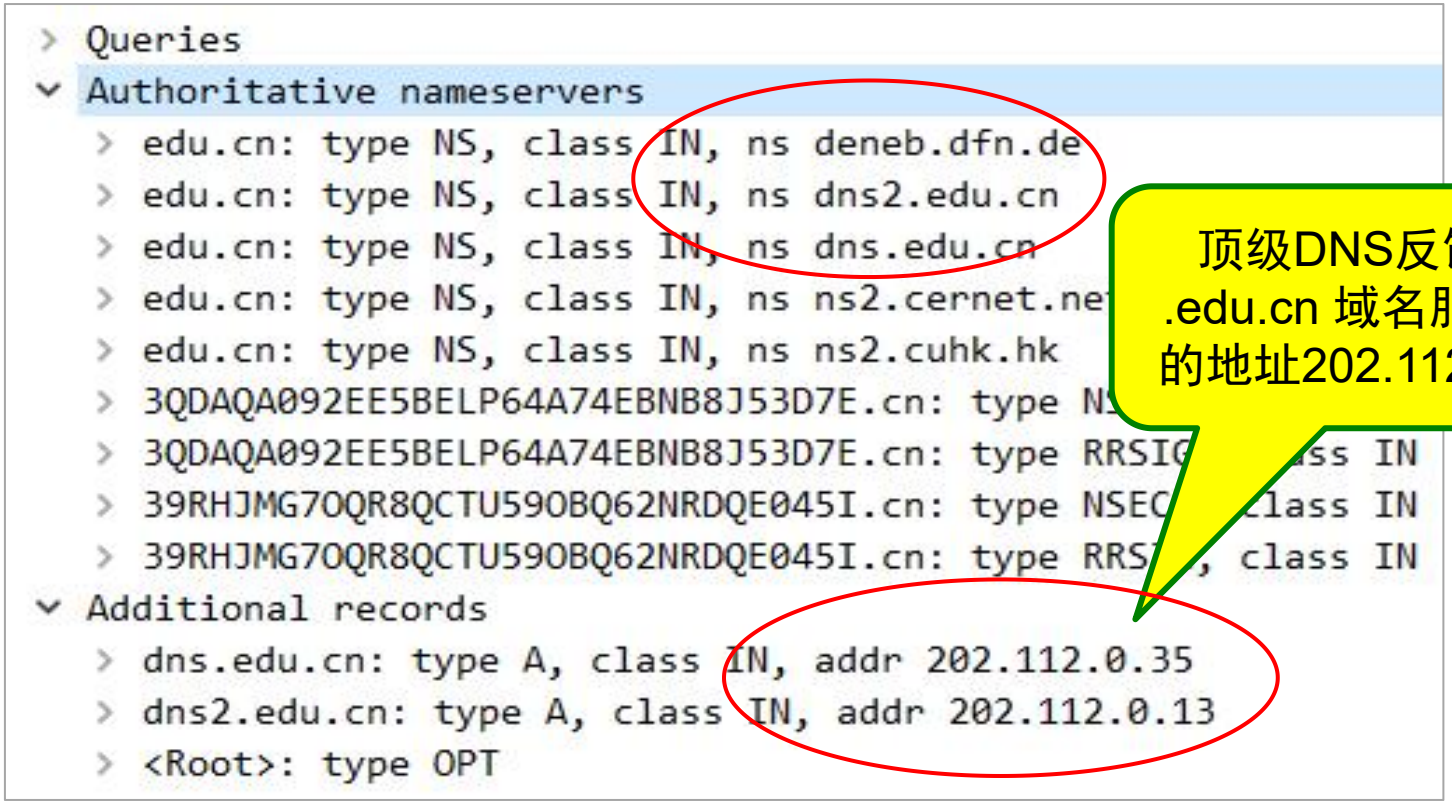
No.	Source	Destination	Protocol	Info
26	192.168.31.100	203.119.28.1	DNS	Standard query 0xaeff A www.hactcm.edu.cn OPT

No.	Source	Destination	Protocol	Info
27	203.119.28.1	192.168.31.100	DNS	Standard query response 0xaeff

A www.hactcm.edu.cn NS deneb.dfn.de NS dns2.edu.cn NS dns.edu.cn NS n…

. cn的顶级域名服务器（203.119.28.1）也不知道www.hactcm.edu.cn对应的IP地址是什么，不过，它发现www.hactcm.edu.cn的二级域名是.edu，而它知道域名服务器dns.edu.cn的IP地址（ 202.112.0.13 ），于是，它告诉了（即应答）本地DNS服务器192.168.31.100。

(27) 203.119.28.1 → 192.168.31.100 顶级DNS .cn → 本地DNS



(28) 192.168.31.100 → 202.112.0.13　　本地DNS → 权限DNS .edu.cn

No.	Source	Destination	Protocol	Info
28	192.168.31.100	202.112.0.13	DNS	Standard query 0xec0f A www.hactcm.edu.cn OPT

本地DNS服务器(192.168.31.100)向202.112.0.13发出解析请求（query）。而202.112.0.13是 .edu.cn域名服务器中的一台（即dns2.edu.cn）。

(29) 202.112.0.13 → 192.168.31.100 权限DNS .edu.cn → 本地DNS

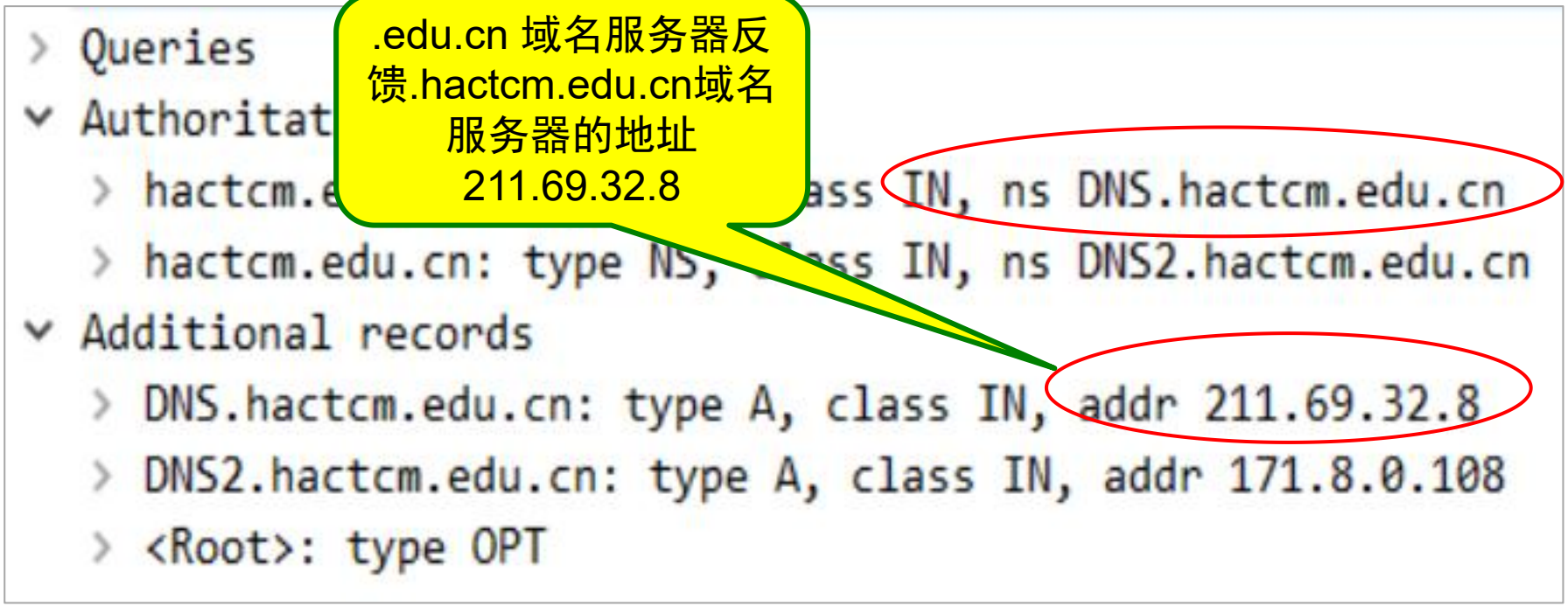
No.	Source	Destination	Protocol	Info
28	192.168.31.100	202.112.0.13	DNS	Standard query 0xec0f A www.hactcm.edu.cn OPT

No.	Source	Destination	Protocol	Info
29	202.112.0.13	192.168.31.100	DNS	Standard query response 0xec0f A www.hactcm.edu.cn

NS DNS.hactcm.edu.cn NS DNS2.hactcm.edu.cn A 211.69.32.8 A 171.8.0.1…

. edu.cn的域名服务器（202.112.0.13）也不知道www.hactcm.edu.cn对应的IP地址是什么，不过，它发现www.hactcm.edu.cn的三级域名是.hactcm，而它知道域名服务器dns.hactcm.edu.cn的IP地址，于是，它告诉了（即应答）本地DNS服务器。

(29) 202.112.0.13 → 192.168.31.100 权限DNS .edu.cn → 本地DNS



(30) 192.168.31.100 → 211.69.32.8　　本地DNS → 权限DNS .hactcm.edu.cn

No.	Source	Destination	Protocol	Info
30	192.168.31.100	211.69.32.8	DNS	Standard query 0x4c2e A www.hactcm.edu.cn OPT

本地DNS服务器(192.168.31.100)向211.69.32.8发出解析请求（query）。而211.69.32.8是 域名服务器dns.hactcm.edu.cn的IP地址。

(31) 211.69.32.8 → 192.168.31.100 权限DNS .hactcm.edu.cn → 本地DNS

No.	Source	Destination	Protocol	Info
30	192.168.31.100	211.69.32.8	DNS	Standard query 0x4c2e A www.hactcm.edu.cn OPT

No.	Source	Destination	Protocol	Info
31	211.69.32.8	192.168.31.100	DNS	Standard query response 0x4c2e

A www.hactcm.edu.cn A 211.69.32.50 NS dns2.hactcm.edu.cn NS dns.hactcm.edu.cn …

域名服务器dns.hactcm. edu.cn（211.69.32.8）就是域名www.hactcm.edu.cn的权限域名服务器，在其数据库中保存有域名www.hactcm.edu.cn对应的IP地址（即一条A记录），经过解析，它告诉了（即应答）本地DNS服务器（192.168.31.100）

(31) 211.69.32.8 → 192.168.31.100 权限DNS .hactcm.edu.cn → 本地DNS

(32) 192.168.31.100 → 192.168.31.50　　本地DNS → 客户机

No.	Source	Destination	Protocol	Info
32	192.168.31.100	192.168.31.50	DNS	Standard query response 0x0002 A www.hactcm.edu.cn A 211.69.32.50

本地DNS服务器(192.168.31.100)向客户机Host-1（192.168.31.50）发回解析请求的结果

www.hactcm.edu.cn的 IP 地址 是 211.69.32.50

DNS服务器的高速缓存

- 为了提高查询效率，每个域名服务器都维护一个高速缓存，存放最近用过的名字以及从何处获得名字映射信息的记录。例如，本地的DNS服务器虽然自身没有存放域名数据库信息，但当它获得一个解析结果后（即取得IP地址后），会将这条记录写入自己的缓存，以备后用。
- 通过利用缓存可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少。
- 为保持高速缓存中的内容正确，域名服务器应为每项内容设置计时器，并处理超过合理时间的项（例如，每个项目只存放1天）。

➢ 为何是“非权威应答”？

```
C:\Users\xuchenggang>nslookup www.hactcm.edu.cn 8.8.8.8
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
名称:    www.hactcm.edu.cn
Address:  211.69.32.50


C:\Users\xuchenggang>nslookup www.hactcm.edu.cn 211.69.32.8
服务器:  QS-DNS
Address:  211.69.32.8

名称:    www.hactcm.edu.cn
Address:  211.69.32.50
```

DNS的故事……

暴风影音断网事件

—— 2009年

所有描述基于当时情况

暴风影音断网事件——发生

- 2009年5月19日22时，工业和信息化部接到电信运营企业报告，自21时起，江苏、河北、山西、广西、浙江等省陆续出现互联网网络故障，部分互联网用户的服务受到影响。
- 2009年 5月20日，工信部发布《情况通报》确认，此次故障原因是由于暴风网站的域名解析系统受到网络攻击出现故障，导致电信运营企业的递归域名解析服务器收到大量异常请求而引发拥塞，造成用户不能正常上网。 工信部确认原因是暴风影音网站受攻击。

暴风影音断网事件——分析

- 20日，工业和信息化部组织相关单位和专家召开了研判会，分析故障原因。会议认为，由于baofeng.com网站的域名解析系统受到网络攻击出现故障，导致电信运营企业的递归域名解析服务器收到大量异常请求而引发拥塞，造成用户不能正常上网。
- 中国电信也已表示，由于暴风影音网站自身域名解析故障，导致中国电信DNS服务器访问量突增，网络处理性能下降。
- 暴风影音网站则表示，经过调查事故原因是DNS域名解析故障，网络故障造成多家网站受到影响，暴风也是受害者之一

暴风影音断网事件——谁是“凶手”

- 【第1张骨牌——以下根据当时的网络报道】
  - 关于网络故障的原因及技术原理，众说纷纭，莫衷一是。 对此，中国互联网络信息中心(CNNIC)副主任兼总工程师李晓东博士认为，引发本次网络故障的第一张骨牌是DNSPOD遭遇网络攻击，而安装有暴风影音的千万台电脑则成为引发整个网络故障连锁反应的重要推力。

暴风影音断网事件——谁是“凶手”

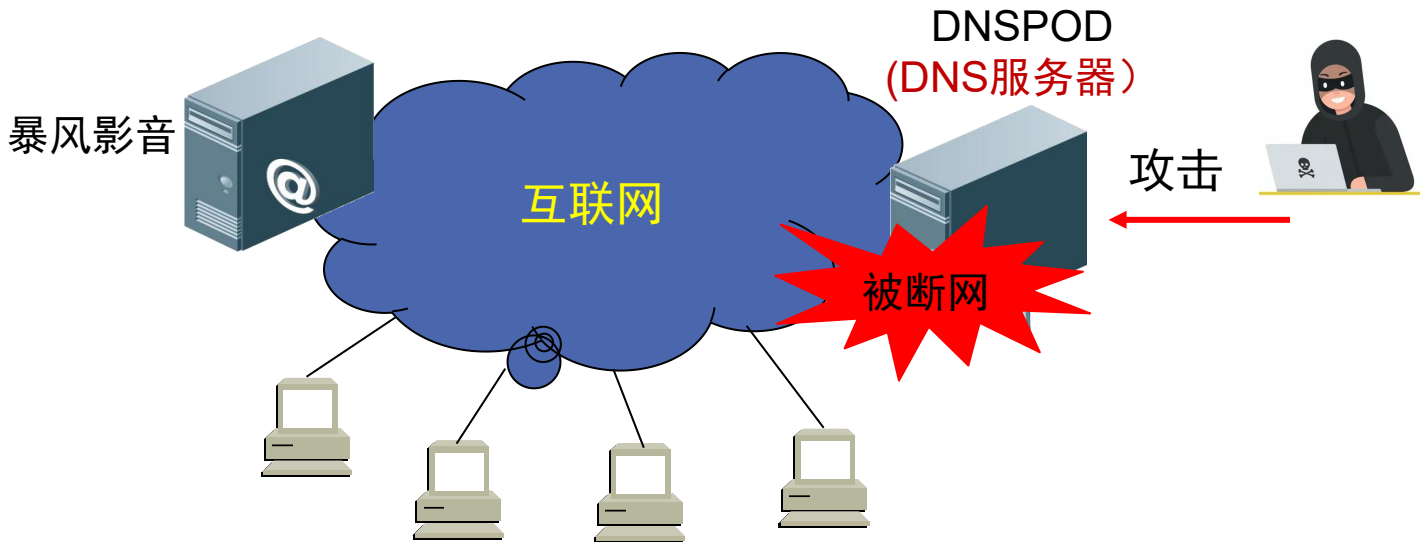
- 交代几个背景资料（基于2009年）
  - DNSPOD：DNSPOD是国内著名的免费域名解析服务提供商，它拥有多台DNS服务器，为全国13万网站提供域名解析服务（相当于权限域名服务器），而此次断网事件的另一主角——国内著名视频播放软件暴风影音，就是其用户之一。（即DNSPOD是解析baofeng.com域名的权限域名服务器）
  - 暴风影音：著名视频播放软件,软件装机量号称达到2亿以上，在中国普及率仅次于腾讯QQ，据称暴风用户同时在线人数达到上千万。Baofeng.com是北京暴风科技公司拥有的域名，用于其公司的各项互联网业务，该域名委托DNSPOD代为运维管理，日常查询量非常大。

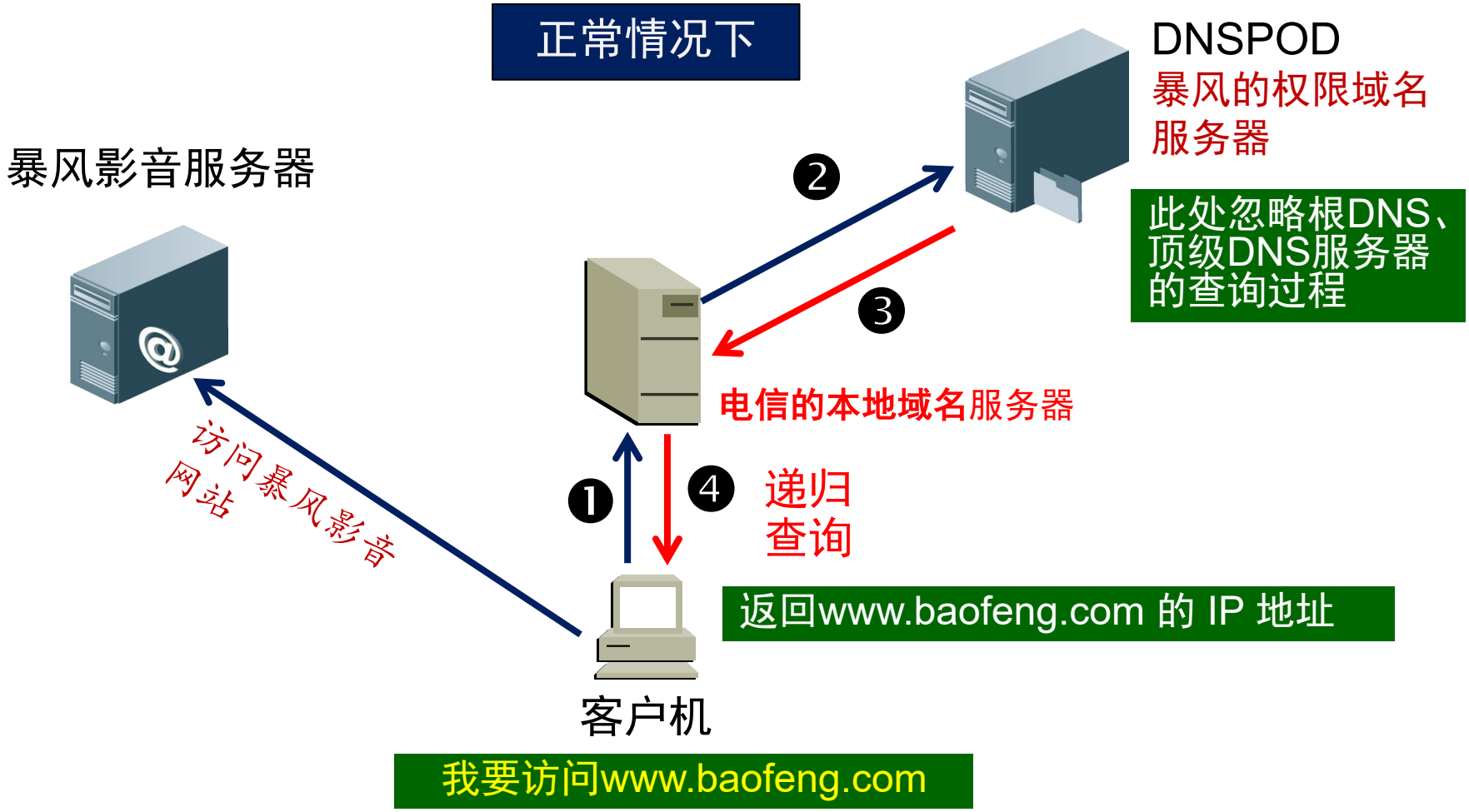
暴风影音断网事件——谁是“凶手”

- 【以下根据当时的网络报道】
  - 李晓东博士表示，此次故障的起源点在于DNSPOD.COM被人恶意大流量攻击，承担DNSPOD.COM网络接入的电信运营商断掉了其网络服务。 这是导致本次网络瘫痪的第一个骨牌。
    - 事件的起点是因为一家游戏私服为了商业利益，利用DDOS攻击另一家游戏私服，未能成功，于是前者转而攻击后者所使用的域名服务器DNSPOD，希望通过此举使对手的域名无法被解析，从而用户无法访问。
    - DDOS攻击造成的巨大流量不仅使DNSPOD的服务器受到影响，而且最终因为网络异常，造成DNSPOD被网络管理部门断网。

暴风影音断网事件—— 谁是“凶手”

- 【以下根据当时的网络报道】
  - 李晓东博士表示，此次故障的起源点在于DNSPOD.COM被人恶意大流量攻击，承担DNSPOD.COM网络接入的电信运营商断掉了其网络服务。 这是导致本次网络瘫痪的第一个骨牌。



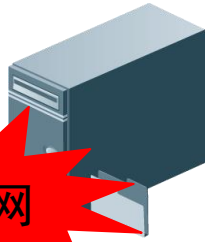

正常情况下
DNSPOD
暴风的权限域名服务器
暴风影音服务器
此处忽略根DNS、顶级DNS服务器的查询过程
2
3
电信的本地域名服务器
访问暴风影音网站
1
4
递归查询
返回www.baofeng.com 的 IP 地址
客户机
我要访问www.baofeng.com

第1张骨牌

暴风的Web服务器

DNSPOD

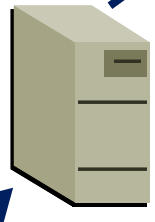
暴风的权限域名服务器



被断网

攻击

电信的本地域名服务器



由于DNSPOD被攻击，造成被断网，本地DNS服务器会告诉客户机解析失败，造成客户机无法再访问暴风影音网站。

客户机1

我要访问www.baofeng.com

暴风影音断网事件——谁是“凶手”

- 【第2张骨牌——以下根据当时的网络报道】
  - 李晓东表示，事实上，第一轮的网络故障早在当晚21时前就已开始。 当时，由于DNSPOD网络服务被中断，致使其无法为包括BAOFENG.COM在内的域名提供域名解析服务，诸多采用DNSPOD服务的网站无法访问
  - 本来，DNSPOD的故障不一定会造成大面积网络故障，但是由于暴风影音的安装量巨大和网络服务的特性，使得暴风影音成为导致此次网络故障的第2张骨牌！

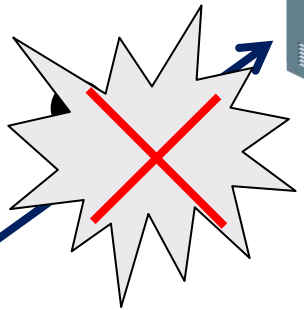
暴风影音断网事件——谁是“凶手”

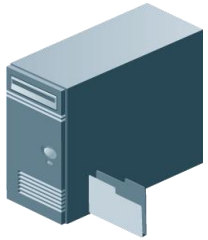
- 【暴漏端倪】
  - 暴风影音含有一个名为stormliv的后台程序，只要用户安装了暴风影音，开机后就会自动运行，而且该程序为了躲避用户删除，使用“服务”的方式自动启动，普通用户很少能将其禁用。
  - 因此，只要一开机，不管是否启动暴风影音主程序，该后台程序都会自动联网，并且访问暴风影音服务器（baofeng.com），进行更新程序，下载广告，报告无法播放文件类型等操作。
  - 不仅如此，当遇到无法连接暴风服务器的情况时，该后台程序会不停的重试连接服务器，毫无意义的消耗本地和网络资源。

第2张骨牌

暴风的Web服务器

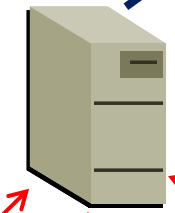
权限域名服务器故障





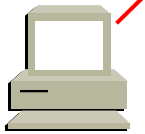
DNSPOD（暴风的权限域名服务器）

电信的本地域名服务器

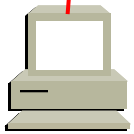


安装暴风影音的用户主机不断向本地DNS发出解析请求！巨量请求！

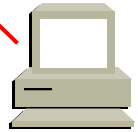
请解析baofeng.com



客户机1

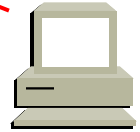


客户机2



客户机3

...



客户机4

安装了暴风影音

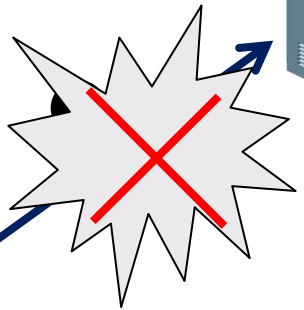
暴风影音断网事件——谁是“凶手”

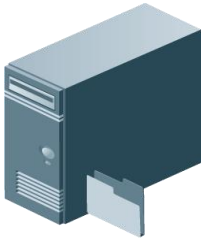
- 【第3张骨牌——以下根据当时的网络报道】
  - 李晓东表示，第3张骨牌就是电信运营商的本地域名服务器。
  - 成千上万安装有暴风影音的电脑发出域名解析请求，不断失败，又不断发起！这些巨量的域名解析请求，拥塞了为这些用户提供上网服务的各地电信运营商的本地域名服务器，导致多个省份的本地域名服务器出现故障甚至无法提供正常服务！
  - 第3张骨牌最终倒掉！

第3张骨牌

暴风的Web服务器

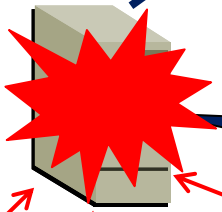
权限域名服务器故障





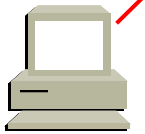
DNSPOD（暴风的权限域名服务器）

电信的本地域名服务器

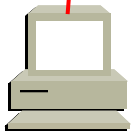


本地域名服务器出现拥塞，不能再为客户机提供解析服务。

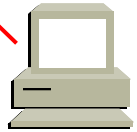
请解析baofeng.com



客户机1

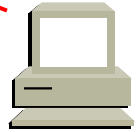


客户机2



客户机3

...



客户机4

暴风影音断网事件——谁是“凶手”

- 【第3张骨牌——以下根据当时的网络报道】
  - 李晓东告诉记者，第3张骨牌是互联网服务的关键环节。
  - 电信运营商的本地域名服务器出现拥塞甚至无法服务后，使用这些本地域名服务器的其他互联网用户也无法上网，造成的结果就是不管用户访问哪个网站都无法得到域名解析的结果，进而导致更大范围内的用户申报网络故障。
  - 最终，出现大面积断网现象。

暴风影音断网事件——总结复盘

- 要重视互联网域名系统的安全性！
  - 域名系统安全“牵一发而动全身”！域名作为广大民众访问互联网的起点和入口，是全球互联网通信的基础。 域名系统作为承载全球亿万域名正常使用的系统，是互联网的基础设施，其作用相当于互联网的中枢神经系统，域名系统的故障会导致互联网陷入瘫痪。
  - 完整的域名系统由递归域名服务系统(即本地域名服务器)、根域名服务系统、顶级域名服务系统以及各级域名服务系统等四个层级构成。广大民众访问一个网站或其他互联网服务时，需要在全球网络中完成对应四个层次的查询。因此，任何一层出现故障，都会导致相应范围的网络应用瘫痪，大到一个国家和地区的网将络全面瘫痪，小到某个网站将无法访问。

暴风影音断网事件——总结复盘

- 要重视互联网域名系统的安全性！
  - 域名系统是一种公开服务，历来是被攻击的对象，从本次网络故障发生的过程来看，相关机构对域名系统的重要性认识不足，重视程度显然不够，安全保障能力比较低。
  - 此次网络故障所涉的三张骨牌都是攻击受害者，估计黑客攻击DNSPOD时也没预料到攻击会产生如此恶劣的后果，最终酿成大范围的网络瘫痪。

暴风影音断网事件——总结复盘

- 要重视互联网域名系统的安全性！
  - 域名系统就像是“空气”，平时我们感觉不到它的存在，但是一旦出现问题，其影响可能是“致命”的。因此，专家建议：
    - 一方面，提供公共域名服务的机构应提高自身安全防御和抗攻击能力；
    - 另一方面，拥有大量用户的互联网软件也应审慎考虑，优化软件安全性，避免一不小心成了分布式拒绝服务攻击(DDOS)的帮凶。
  - 专家呼吁：希望大家携手共同努力，重视并加大各个层级域名系统保护力度，为亿万网民营造一个“安全、可靠”的互联网环境。

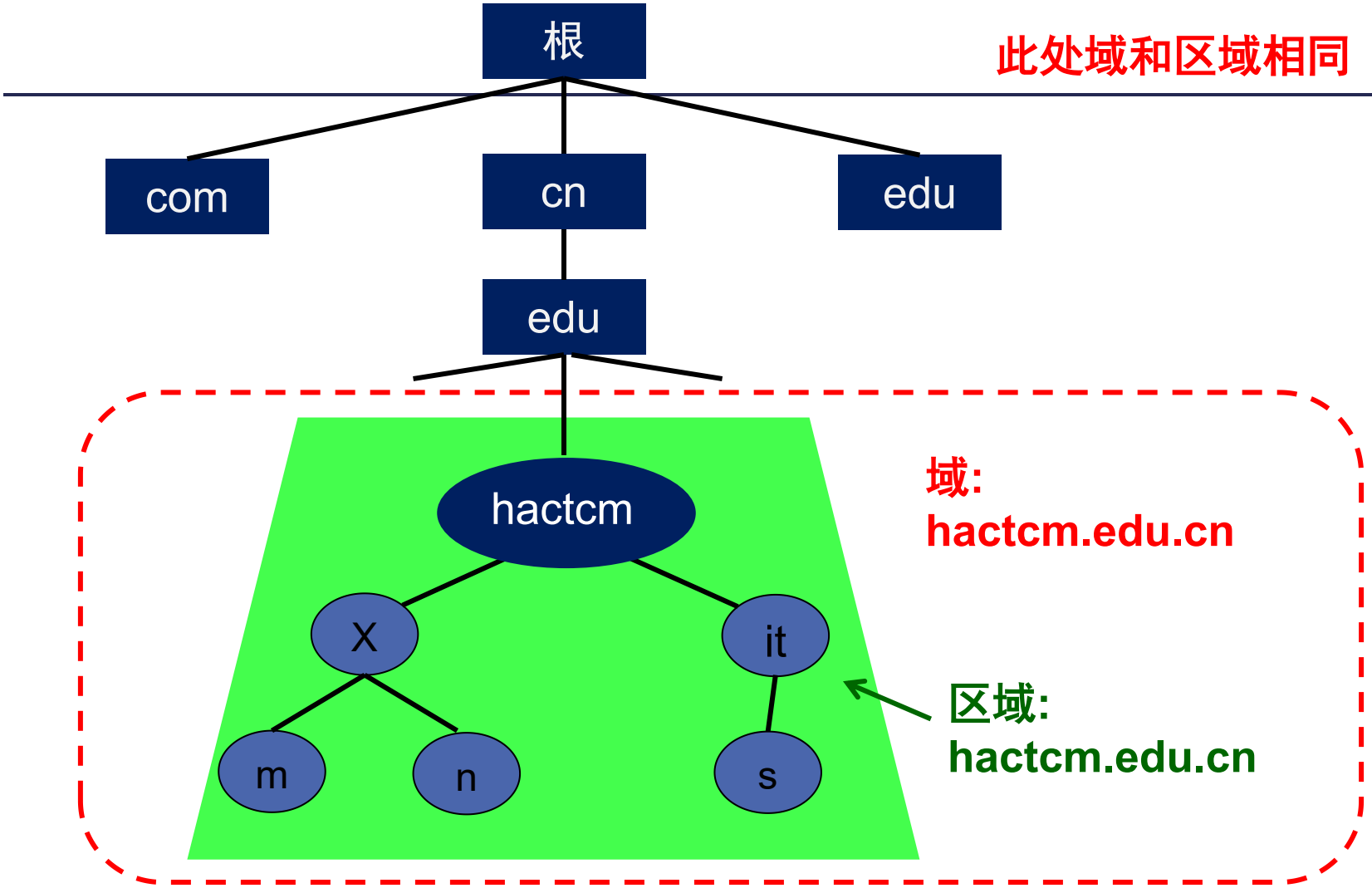
暴风影音断网事件

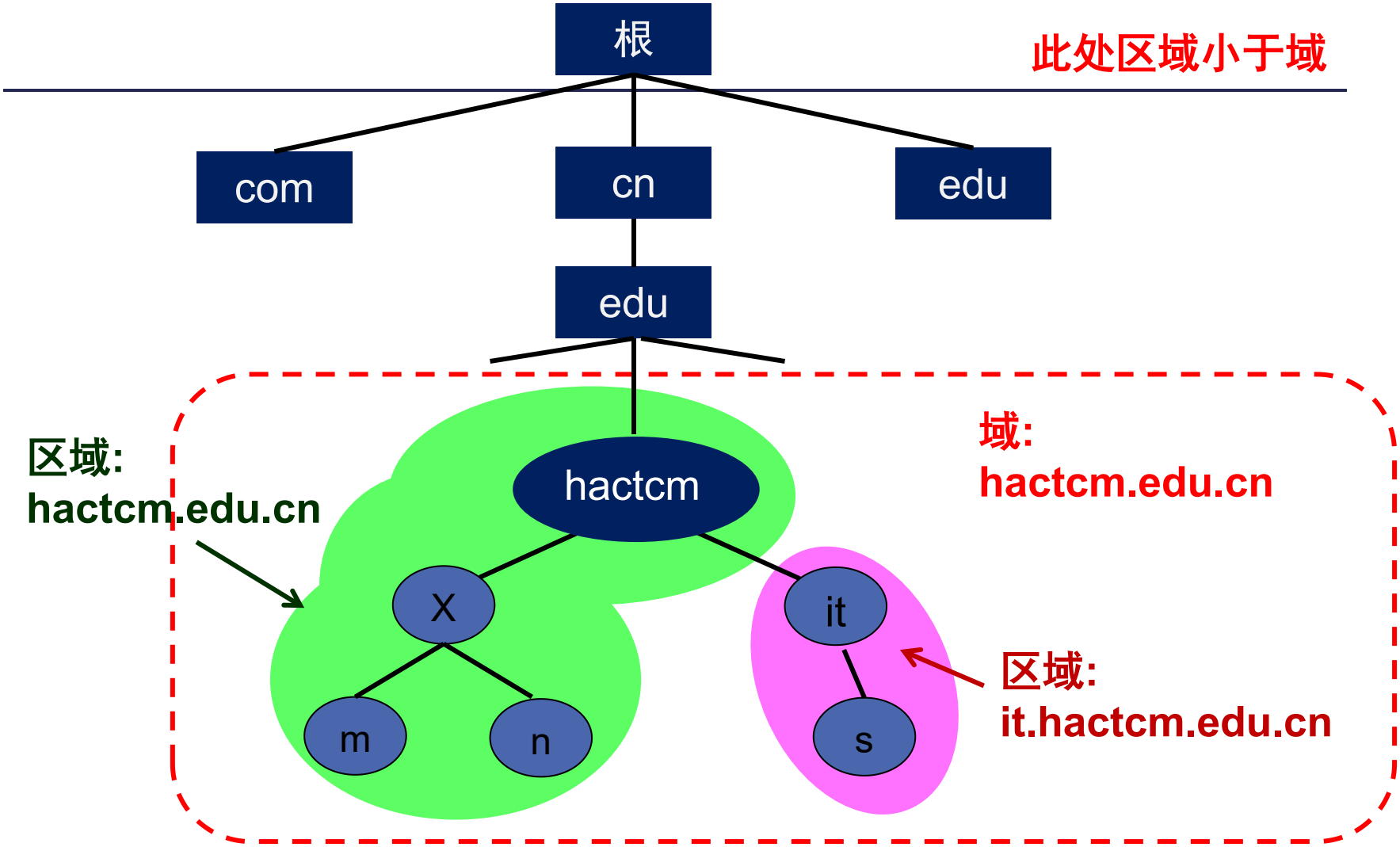
完

四、DNS的区域

4.DNS的区域

- 为了分散整个DNS系统的负荷，将DNS域名空间划分为区域（zone）来进行管理。
- DNS服务器是通过区域（zone）来管理域名空间的，而不是以域为单位来管理域名空间的。


根
此处域和区域相同
com
cn
edu
edu
hactcm
域:
hactcm.edu.cn
X
it
区域:
hactcm.edu.cn
m
n
s


根
此处区域小于域
com
cn
edu
edu
区域:
hactcm.edu.cn
hactcm
域:
hactcm.edu.cn
X
it
m
n
s
区域:
it.hactcm.edu.cn

4.DNS的区域

- 每个区域都是自我管辖的项目。区域中可以有一个或多个子域；
- 每个区域至少有一个DNS服务器。
- 每个区域中通常有一系列的记录，用来表示具体的域名和IP地址的映射关系；
- 搭建DNS服务器时，必须先建立区域（zone），然后再根据需要在区域中建立子域以及在区域或子域中添加记录。这样才能完成其解析工作。

4.DNS的区域

- DNS区域按照解析方式的不同可划分为：
  - 正向查找区域（用于域名到IP地址的映射）
    - 当DNS客户端请求解析某个域名时，DNS服务器在正向查找区域中进行查找，并返回给DNS客户端对应的IP地址；
  - 反向查找区域（用于IP地址到域名的映射）
    - 当DNS客户端请求解析某个IP地址时，DNS服务器在反向查找区域中进行查找，并返回给DNS客户端对应的域名；

五、DNS的记录

5.DNS的记录

- 常见的记录类型有以下几种：
  - 主机记录（A）
  - AAAA记录
  - 别名记录（CNAME）
  - 邮件交换记录（MX）
  - NS记录
  - 起始授权机构记录（SOA）
  - PTR记录
  - SRV记录

5.DNS的记录

- 主机记录（A）

  主机记录（A）在DNS区域中通常完成计算机名字到IP地址的映射。

- AAAA记录

  AAAA资源记录类型用来将一个合法域名解析为IPv6地址，与IPv4所用的A资源记录类型相兼容。

- 别名记录（CNAME）

  别名记录（CNAME）也被称为规范名称。这种记录允许操作者将多个名称映射到同一台计算机。

5.DNS的记录

- 邮件交换记录（MX）

  邮件交换记录（MX）用于电子邮件程序发送邮件时，根据收信人的地址后缀来定位邮件服务器。

- NS记录

  NS记录是域名服务器记录，用于标识解析该域或其它域（例如子域）各种主机记录的域名服务器。

- SOA记录

  起始授权机构记录（SOA），是用来识别域名中由哪一个域名服务器负责信息授权。

5.DNS的记录

- PTR记录

  PTR记录用于IP地址解析到域名，它被视为反向A记录。

- SRV记录

  SRV记录是DNS服务器的数据库中支持的一种资源记录的类型，它记录了哪台计算机提供了哪个服务。

六、DNS的数据库文件

6.DNS的数据库文件

- 在DNS数据库文件中，包含着“域名--IP地址”的对应数据以及其它有关数据，这些数据称为资源记录（Resource Record）。
- DNS的数据库文件包括以下几类。
  - 区域文件
  - 缓存文件
  - 正向、反向查询文件
  - 引导文件

6.DNS的数据库文件

- 区域文件（zone file）
  - 区域文件中保存着DNS服务器所管辖区域内的有关资源记录。
  - 在Windows Server 2012中，当利用“DNS管理器”新建区域时，区域文件便会自动生成，默认的文件名是“区域名.dns”。
  - 在BIND中，区域文件是由管理员配置并定义的。

6.DNS的数据库文件

- 缓存文件
  - 缓存文件和缓存是不同的两回事。
  - 高速缓存中保存的是已查到的数据，以便下次能够快速查询相同的数据。
  - 缓存文件中保存的是根域中DNS服务器的“域名--IP地址”的对应数据。
  - 每台DNS服务器中的缓存文件都应该是一样的，是DNS服务器查询外界Internet主机的IP地址时用的。

6.DNS的数据库文件

- 正向、反向查询文件
  - 进行名字解析时，一般是用名字来查询IP地址，这称作正向查询。
  - 用IP地址来查询名字，称为反向查询。
  - 正向查询和反向查询都需要事先建立一个特殊的查询区域和相应的查询文件，分别将这种文件称作正向查询文件和反向查询文件。

6.DNS的数据库文件

- 引导文件
  - 引导文件是一个文本文件，负责存储DNS服务器的启动信息。
  - 使用文本格式的命令和说明来设置一台DNS服务器。
  - 引导文件只用在BIND建设的DNS服务器上。

七、在Windows Server上实现DNS

7.在Windows Server上实现DNS

- Windows Server 2012系统已经内置了DNS服务软件，只需要开启即可。
- 实现DNS服务的具体流程如下。
  - 新建正向查找区域。
  - 创建A记录，并验证其可用性。
  - 创建CNAME记录，并验证其可用性。
  - 新建反向查找区域。
  - 创建PTR记录，并验证其可用性。

八、在Linux上实现DNS

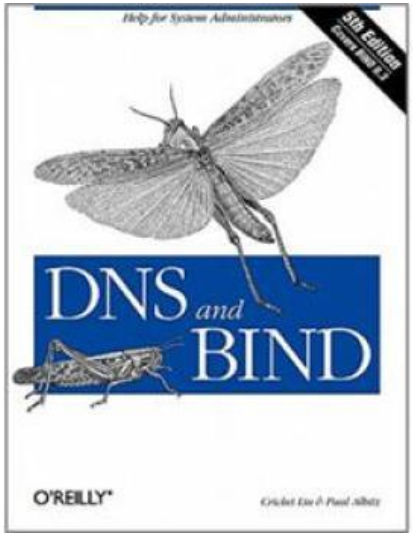
8.在Linux上实现DNS

BIND简介

- Linux下构建DNS服务器通常是使用BIND来实现的。
- BIND是Berkeley Internet Name Domain Service的简称，是一款实现DNS服务器的开源服务软件。
- BIND原本是美国DARPA资助伯里克大学（Berkeley）开设的一个研究生课题研究，后来经过多年的变化发展，已经成为世界上使用最为广泛的DNS服务器软件，目前Internet上绝大多数的DNS服务器都是用BIND来构建的。

8.在Linux上实现DNS

CentOS + BIND



8.在Linux上实现DNS

- 思考：
  - 配置DNS服务器时，是否需要虚拟机接入互联网？

8.在Linux上实现DNS

- BIND中的软件包
  - BIND服务有关的软件包有如下几个：
  - **bind**
    - BIND服务器端软件，即BIND 主程序。
  - **bind-chroot**
    - 为BIND提供chroot机制的软件包，将BIND设定文件和程序限制在虚拟根目录下。如果不使用chroot保护BIND，可以不安装，但是推荐安装。为bind提供一个伪装的根目录以增强安全性（将“/var/named/chroot/文件夹作为BIND的根目录”）

8.在Linux上实现DNS

- BIND中的软件包
  - BIND服务有关的软件包有如下几个：
  - **bind-utils**
    - 客户端搜索主机名的相关命令，提供nslookup及dig等测试工具
  - **bind-libs**
    - BIND相关的库文件

8.在Linux上实现DNS

- 使用yum命令安装BIND软件包，命令格式是：

```
yum -y install bind bind-chroot bind-utils bind-libs
```

8.在Linux上实现DNS

- 思考：
  - 安装BIND时，DNS服务器是否需要配置本地DNS地址？

```
yum -y install bind bind-chroot bind-utils bind-libs
```

8.在Linux上实现DNS

- 使用yum命令安装BIND软件包，命令格式是：

```
[root@localhost ~]# yum -y install bind bind-chroot bind-utils bind-libs
已加载插件：fastestmirror
base
extras
updates
(1/4): extras/7/x86_64/primary_db
(2/4): base/7/x86_64/group_gz
(3/4): base/7/x86_64/primary_db
(4/4): updates/7/x86_64/primary_db
Determining fastest mirrors
 * base: mirror.neu.edu.cn
 * extras: ftp.sjtu.edu.cn
 * updates: ftp.sjtu.edu.cn
正在解决依赖关系
--> 正在检查事务
---> 软件包 bind.x86_64.32.9.9.4-29.el7_2.3 将被 安装
---> 软件包 bind-chroot.x86_64.32.9.9.4-29.el7_2.3 将被 安装
---> 软件包 bind-libs.x86_64.32.9.9.4-29.el7_2.3 将被 安装
--> 正在处理依赖关系 bind-license = 32:9.9.4-29.el7_2.3，它被软件包 32:bind-libs-9.9
---> 软件包 bind-utils.x86_64.32.9.9.4-29.el7_2.3 将被 安装
--> 正在检查事务
---> 软件包 bind-license.noarch.32.9.9.4-18.el7 将被 升级
```

8.在Linux上实现DNS

- 使用yum命令安装BIND软件包，命令格式是：

```
================================================================================
 Package                架构      版本                      源          大小
================================================================================
正在安装:
 bind                   x86_64    32:9.9.4-29.el7_2.3       updates     1.8 M
 bind-chroot            x86_64    32:9.9.4-29.el7_2.3       updates      83 k
 bind-libs              x86_64    32:9.9.4-29.el7_2.3       updates     1.0 M
 bind-utils             x86_64    32:9.9.4-29.el7_2.3       updates     200 k
为依赖而更新:
 bind-libs-lite         x86_64    32:9.9.4-29.el7_2.3       updates     724 k
 bind-license           noarch    32:9.9.4-29.el7_2.3       updates      82 k

事务概要
================================================================================
安装  4 软件包
升级             ( 2 依赖软件包)

总下载量：3.8 M
```

8.在Linux上实现DNS

- 安装完成后会生成以下文件

/etc/named.conf	bind主配置文件
/etc/named.rfc1912.zones	区域声明文件
/var/named/named.localhost	区域配置样例文件
/var/named/named.ca	根域名文件

8.在Linux上实现DNS

- BIND主要有三类配置文件
  - （1）BIND的主配置文件
    - BIND主配置文件即 /etc/named.conf，里面有BIND的全局设置；
  - （2）区域声明文件
    - 区域声明文件即 /etc/named.rfc1912.zones，里面列举了本机中各个区域记录配置文件的位置/类型/性质。实际上，在主配置文件named.conf中，使用“Include "/etc/named.rfc1912.zones"”语句来调用区域声明文件。

8.在Linux上实现DNS

- BIND主要有三类配置文件
  - （3）区域配置文件
    - 一个DNS服务器中可以设置多个区域配置文件，每一个区域配置文件指明了本DNS服务器所负责解析的某个区域中IP 和域名的对应关系，即各种记录内容，例如A记录、NS记录等。
    - 区域配置文件存放在 /var/named目录下。

8.在Linux上实现DNS

- 查看BIND的主配置文件
  - 该文件存放在 /etc 目录中，使用cat命令进行查看

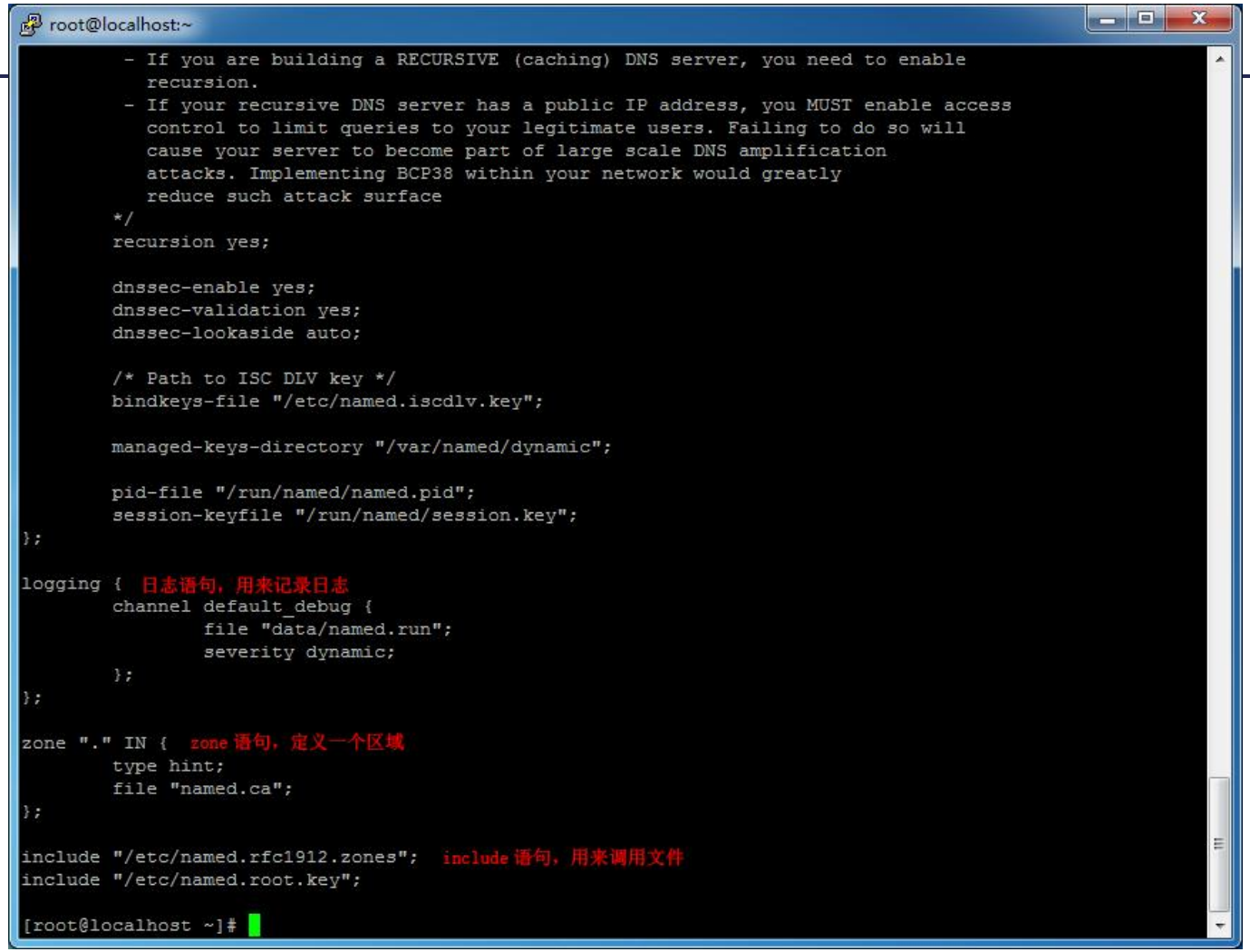
```
# cat /etc/named.conf
```

```
[root@localhost ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {    option 语句
        listen-on port 53 { 127.0.0.1; };  侦听地址（IPv4）
        listen-on-v6 port 53 { ::1; };   侦听地址（IPv6）
        directory       "/var/named";    工作目录
        dump-file       "/var/named/data/cache_dump.db";  缓存文件
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };  访问控制

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;  递归查询

        dnssec-enable yes;
        dnssec-validation yes;
```


root@localhost:~
- If you are building a RECURSIVE (caching) DNS server, you need to enable
recursion.
- If your recursive DNS server has a public IP address, you MUST enable access
control to limit queries to your legitimate users. Failing to do so will
cause your server to become part of large scale DNS amplification
attacks. Implementing BCP38 within your network would greatly
reduce such attack surface
*/
recursion yes;
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";
managed-keys-directory "/var/named/dynamic";
pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";
};
logging { 日志语句，用来记录日志
channel default_debug {
file "data/named.run";
severity dynamic;
};
};
zone "." IN { zone 语句，定义一个区域
type hint;
file "named.ca";
};
include "/etc/named.rfc1912.zones"; include 语句，用来调用文件
include "/etc/named.root.key";
[root@localhost ~]#

8.Linu

- BIND配

表 5-03 BIND 配置文件语句

命令语句	解释说明
acl	定义 IP 地址访问控制列表
controls	宣告认得 utility 使用的控制通道（channel）
include	包含一个文件
key	设置密钥信息，它应用在通过 TSIG 进行授权和认证配置中
logging	设置日志服务器，和日志信息的发送地
options	控制服务器的全局配置选项和其它语句设置默认值
server	在一个单服务器基础上设置特定的配置选项
trusted-keys	定义信任的 DNSSED 密钥
view	定义一个视图
zone	定义一个域

8.在Linux上实现DNS

- 查看根域配置文件named.ca的内容
  - 在主配置文件named.conf中，定义了根域“.”，其对应的区域配置文件为named.ca。当DNS服务器无法解析某个域名时，就可以根据named.ca文件中的记录信息，向根域名服务器发出查询请求。
  - named.ca文件存放在 /var/named 目录中，使用 vi命令进行查看

```
;; ANSWER SECTION:
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3600000 IN      A       198.41.0.4
a.root-servers.net.     3600000 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3600000 IN      A       192.228.79.201
c.root-servers.net.     3600000 IN      A       192.33.4.12
d.root-servers.net.     3600000 IN      A       199.7.91.13
d.root-servers.net.     3600000 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3600000 IN      A       192.203.230.10
f.root-servers.net.     3600000 IN      A       192.5.5.241
f.root-servers.net.     3600000 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3600000 IN      A       192.112.36.4
h.root-servers.net.     3600000 IN      A       128.63.2.53
h.root-servers.net.     3600000 IN      AAAA    2001:500:1::803f:235
i.root-servers.net.     3600000 IN      A       192.36.148.17
i.root-servers.net.     3600000 IN      AAAA    2001:7fe::53
j.root-servers.net.     3600000 IN      A       192.58.128.30
j.root-servers.net.     3600000 IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     3600000 IN      A       193.0.14.129
k.root-servers.net.     3600000 IN      AAAA    2001:7fd::1
l.root-servers.net.     3600000 IN      A       199.7.83.42
l.root-servers.net.     3600000 IN      AAAA    2001:500:3::42
m.root-servers.net.     3600000 IN      A       202.12.27.33
m.root-servers.net.     3600000 IN      AAAA    2001:dc3::35
```

所有的根DNS服务器的相关记录

8.Linux下实现BIND

- 修改主配置文件中的侦听地址
  - 配置named.conf，修改侦听地址，并允许所有主机可以访问。
  - 在文件中找到：

```
listen-on port 53 { 127.0.0.1; };
allow-query       { localhost; };
```

  - 改为：

```
listen-on port 53 { any; };
allow-query       { any; };
```

8.Linux下实现BIND

- 在主配置文件中定义查找区域
  - 在named.conf中添加以下内容，定义一个区域名称为“xuchenggang.net”的正向查找区域，区域类型为主要区域。

```
zone "xuchenggang.net" IN {
// 定义一个区域名称为“xuchenggang.net”的正向查找区域；
        type master;      // 区域类型为主要区域
        file "xuchenggang.net.zone";
// 将该区域的区域配置文件命名为“ xuchenggang.net.zone”。注意，此处为相对路径，即表示该文件将被放置在 /var/named下，也可写成绝对路径；
        allow-update { none; };
};
```

8.Linux下实现BIND

- 注意，在上一步骤中，我们只是在主配置文件（named.conf）文件中定义（即声明）了一个区域，并且定义了这个区域的配置文件名。但是，相应的区域配置文件并没有创建。
- 接下来要创建区域配置文件xuchenggang.net.zone并在文件中添加“域名—IP地址”的有关记录。
- 注意，这个文件要创建在 /var/named目录中。

```
# vi /var/named/xuchenggang.net.zone
```

8.Linux下实现BIND


```
$TTL 1D
@       IN SOA dns.xuchenggang.net.  root.xuchenggang.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@               IN                      NS                      dns.xuchenggang.net.
dns             IN                      A                       192.168.31.100
ftp             IN                      A                       192.168.31.200
www             IN                      A                       192.168.31.201
mail            IN                      A                       192.168.31.202
web             IN                      CNAME                   www.xuchenggang.net.
@               IN                      MX  10                   mail.xuchenggang.net.
```

- 对区域配置文件的说明：
  - @ 代表相应的域名，例如此处代表 xuchenggang.net，表示一个区域记录定义的开始。
  - IN表示后面的数据使用的是INTERNET标准。
  - SOA 表示授权开始，其后面跟权威DNS服务器的主机名称（FQDN），此处为“dns.xuchenggang.net.”。 **注意，最后面的“.”不能丢，因为此处的“.”表示一个完整主机名称的结束，如果不加点，则系统会默认在原主机名称后再加上“xuchenggang.net”，即变成了“dns.xuchenggang.net.xuchenggang.net”。**

8.Linux下实现BIND

- 对区域配置文件的说明：
  - root.xuchenggang.net.表示管理员邮件地址。注意，这里的邮件地址中用.来代替常见的邮件地址中的@，因为@ 用来表示本区域。
  - serial：定义正向解析区域的序列号。
  - refresh：定义自动刷新间隔时间。
  - retry：定义刷新重试时间。
  - expire：定义数据的有效期限。
  - minimum：定义最小默认的生存时间。

8.Linux下实现BIND

- 对区域配置文件的说明：
  - NS：表示记录类型为NS记录。
  - A：表示记录类型为A记录。
  - MX：表示记录类型为MX记录，后面紧跟的数值为优先级数值。
  - CNAME：表示记录类型为别名记录。
  - www、mail、ftp：表示主机名。

8.Linux下实现BIND

- 定义一个区域名称为“1.168.192.in-addr.arpa”的反向查找区域。
  - 在named.conf中添加以下内容，定义一个反向查找区域。

```
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "192.168.1.zone";
};
```

8.Linux下实现BIND

- 配置区域文件
  - 区域文件192. 168. 1. zone的配置示例：

```
$TTL 1D
@       IN     SOA    example.sy.com. root.sy.com. (
                                        0        ; serial
                                        1D       ; refresh
                                        1H       ; retry
                                        1W       ; expire
                                        3H )     ; minimum
@     IN      NS     example.sy.com.
1     IN      PTR    example.sy.com.
2     IN      PTR    www.sy.com.
3     IN      PTR    mail.sy.com.
4     IN      PTR    ftp.sy.com.
```

8.Linux下实现BIND

- 为了保证BIND配置文件和区域文件的格式不会出错，输入以下命令可检查配置文件的格式是否正确。
  - 检查named.conf格式的命令为：named-checkconf 配置文件名（包含路径）

```
# named-checkconf /etc/named.conf
```

  - 检查区域文件格式的命令为：named-checkzone 区域名称 区域文件名称（包含路径）

```
# named-checkzone sy.com /var/named/sy.com.zone
# named-checkzone 1.168.192.in-addr.arpa /var/named/192.168.1.zone
```

九、DNS的高级功能

9.DNS高级功能

- DNS高级功能主要有以下几种。
  - ACL（地址匹配列表）
  - DNS转发

9.DNS高级功能

- ACL是访问控制列表（Access Control List），在DNS中ACL是用来进行访问控制的地址匹配列表，其主要用来限制DNS服务器的访问和数据的传输，这对DNS的安全有一定的保障。
- 在BIND中，可使用ACL语句用来添加匹配的地址列表。

9.DNS高级功能

- 定义了地址匹配列表后，可在以下语句中使用。

语句	说明
allow-query	指定哪些主机或网络可以查询本服务器或区。
allow-transfer	指定哪些主机允许和本地服务器进行域传输。
allow-recursion	指定哪些主机可以进行递归查询
allow-update	指定哪些主机允许为主域名服务器提交动态 DNS 更新。
blackhole	指定不接收来自哪些主机的查询请求和地址解析。
match-clients	指定哪些来源地址，进行匹配。
match-destinations	指定哪些目的地址，进行匹配。

9.DNS高级功能

- 限制只有192.168.1.0/24和10.0.0.0/24查询本地服务器的所有区域信息。
  - 不使用acl语句时，named.conf的配置为：

```
options {
......
allow-query { 192.168.1.0/24; 10.0.0.0/24; };
......
};
```

9.DNS高级功能

- 使用acl语句时，named.conf的配置为：

```
acl name1 {
  192.168.1.0/24;
  10.0.0.0/24;
};
options {
......
allow-query { name1; };
......
};
```

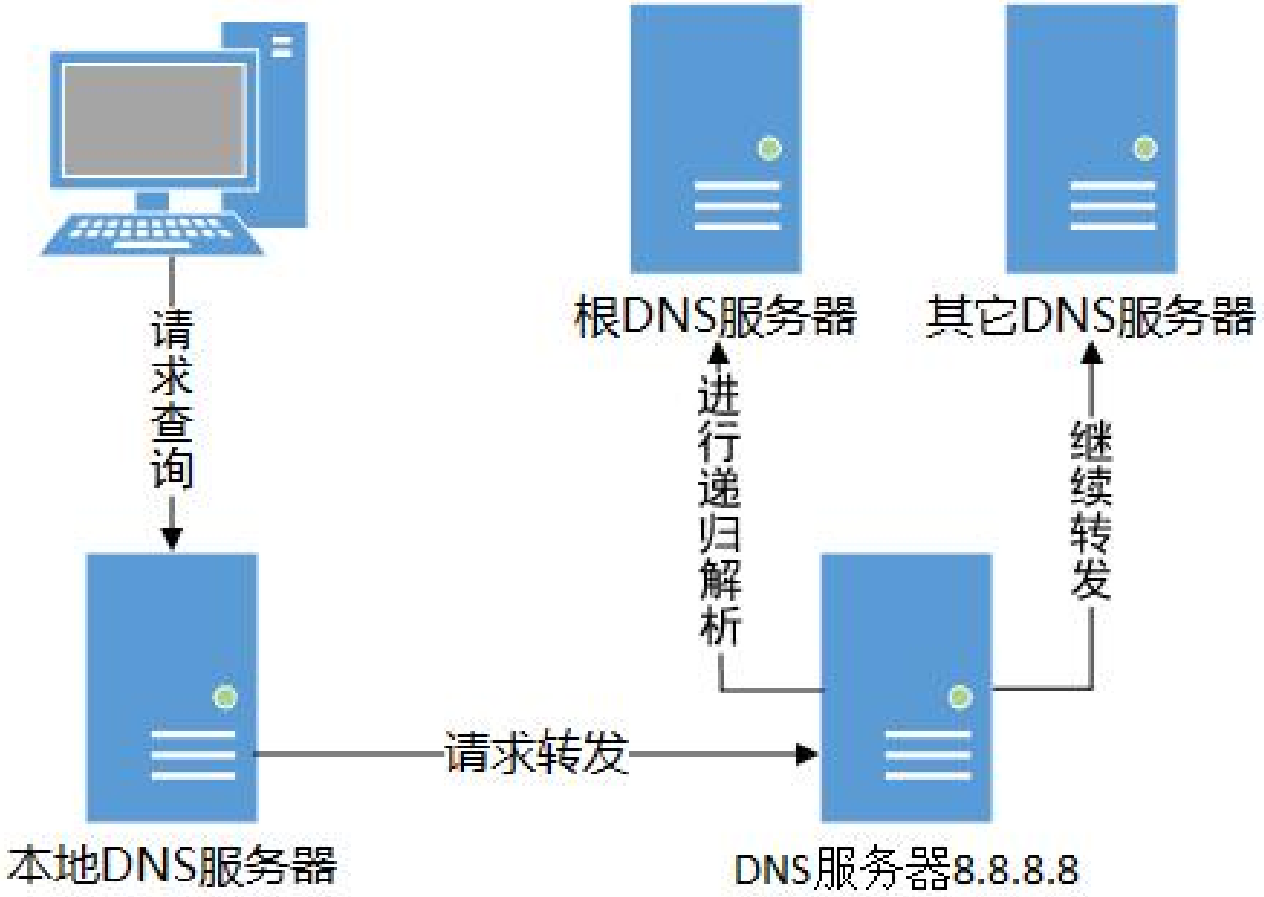
9.DNS高级功能

- DNS转发就是DNS服务器将来自DNS客户端或者服务器的DNS请求，转发到其他DNS服务器进行解析的过程。
- 当本地DNS服务器无法提供所需要的数据时，可以将DNS请求转发到别的DNS服务器，然后将查询的结果返回给DNS客户端，并保存在缓存中。

9.DNS高级功能

- 完全转发与区域转发
  - 完全转发是指DNS服务器将所有的查询请求都转发给其他的DNS服务器进行解析。
  - 区域转发则是将某些特定的区域的查询请求进行转发，而其他区域的查询请求仍使用递归解析或者迭代解析。

DNS转发


根DNS服务器
其它DNS服务器
请求查询
进行递归解析
继续转发
请求转发
本地DNS服务器
DNS服务器8.8.8.8

十、多链路DNS智能解析

10. 智能DNS

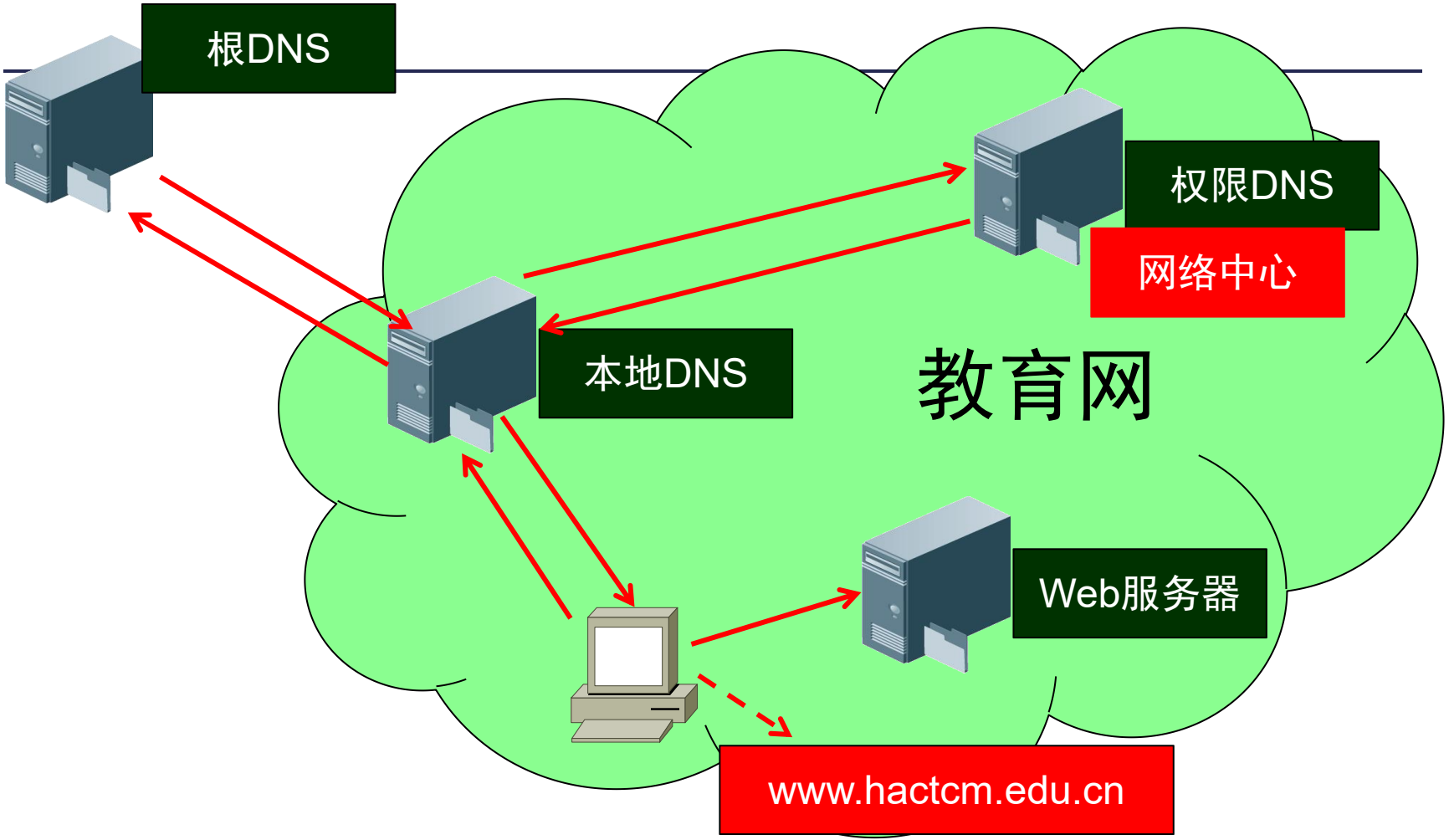
智能DNS的含义

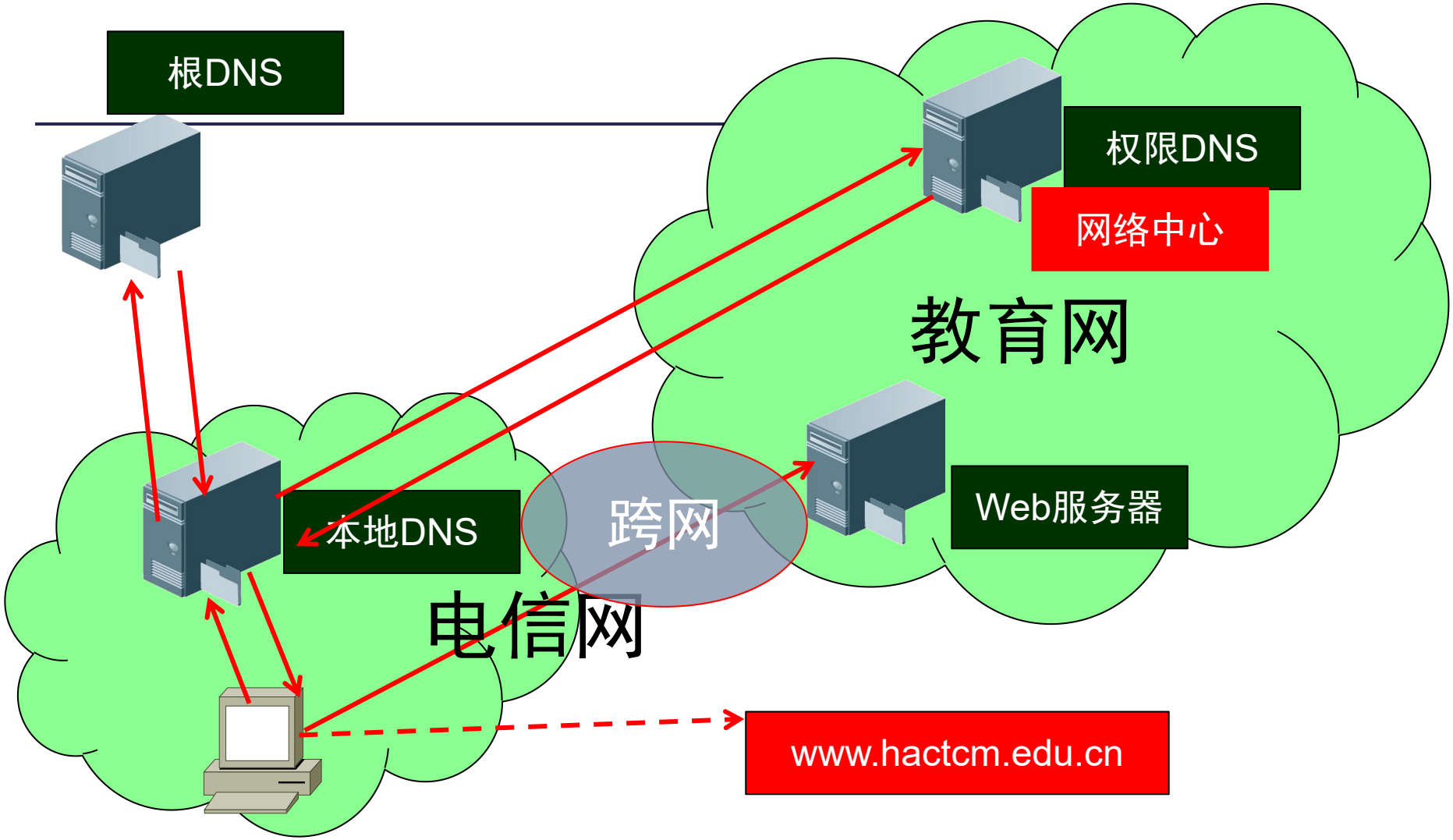
- 智能DNS解析是针对电信、联通、教育网互联互通不畅的问题推出的一种DNS解决方案。
- 具体实现是：把同样的域名如hntcm.cn的A记录分别设置指向部署于电信、联通、教育网的相应服务器的IP；
- 当电信的客户访问时，智能DNS会自动判断访问者来路，并返回相应的部署在电信的服务器的IP地址；
- 当联通的客户访问时会自动返回部署在联通的服务器IP地址；当教育网的客户访问时，会返回部署在教育网的服务器IP地址。

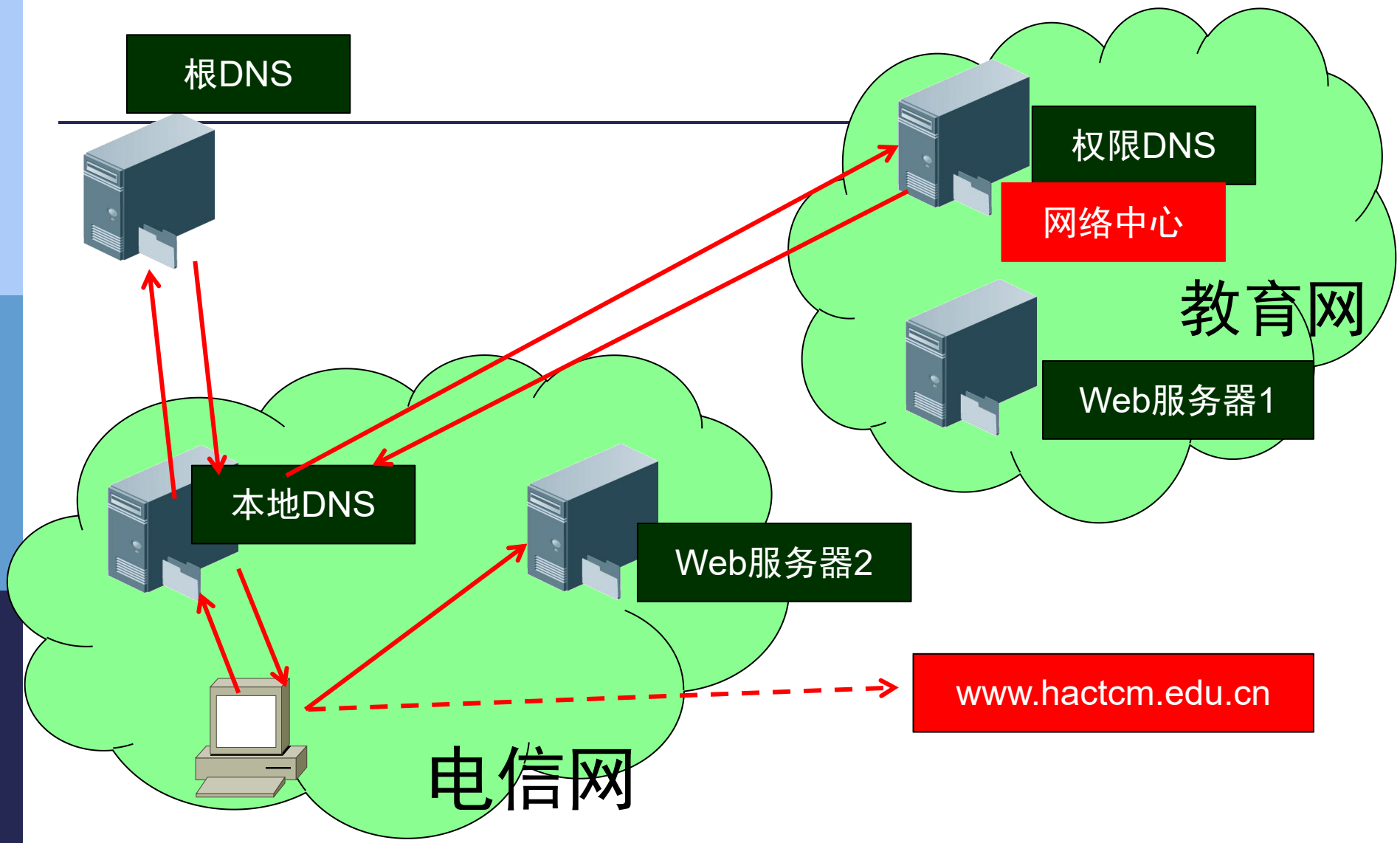
10. 智能DNS

智能DNS的含义

- 也就是说，智能DNS（多链路解析）就是让DNS服务器根据不同请求的IP地址或者所在区域，返回不同的解析结果给DNS客户端。
- 这样，就可以避免联通的客户去访问电信的网络，以及电信的客户去访问联通的网络等现象，很好的解决了客户跨网访问不畅的问题。当然亦可加入多IP，由智能DNS自动“选路”。

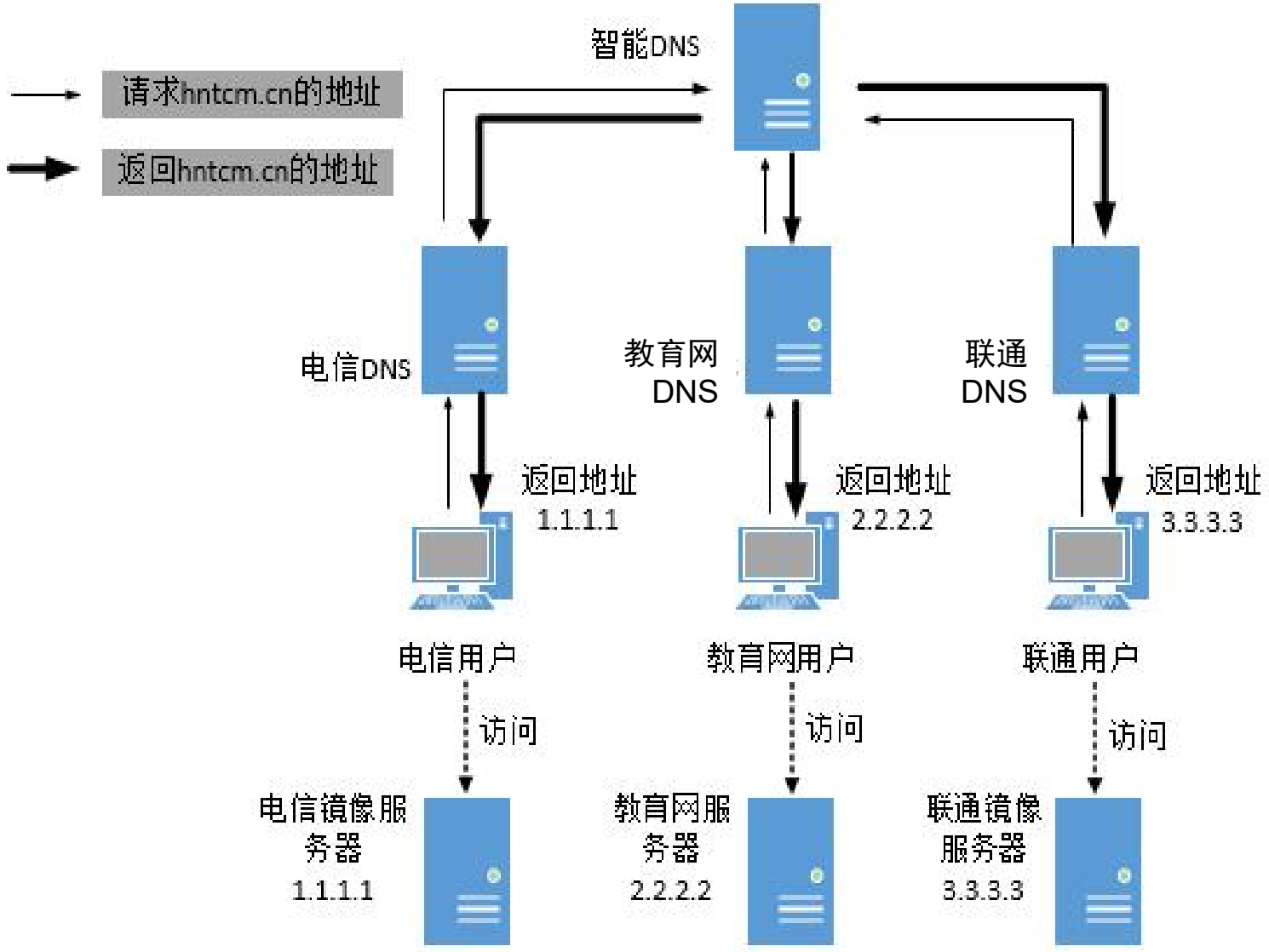

根DNS
权限DNS
网络中心
本地DNS
教育网
Web服务器
www.hactcm.edu.cn

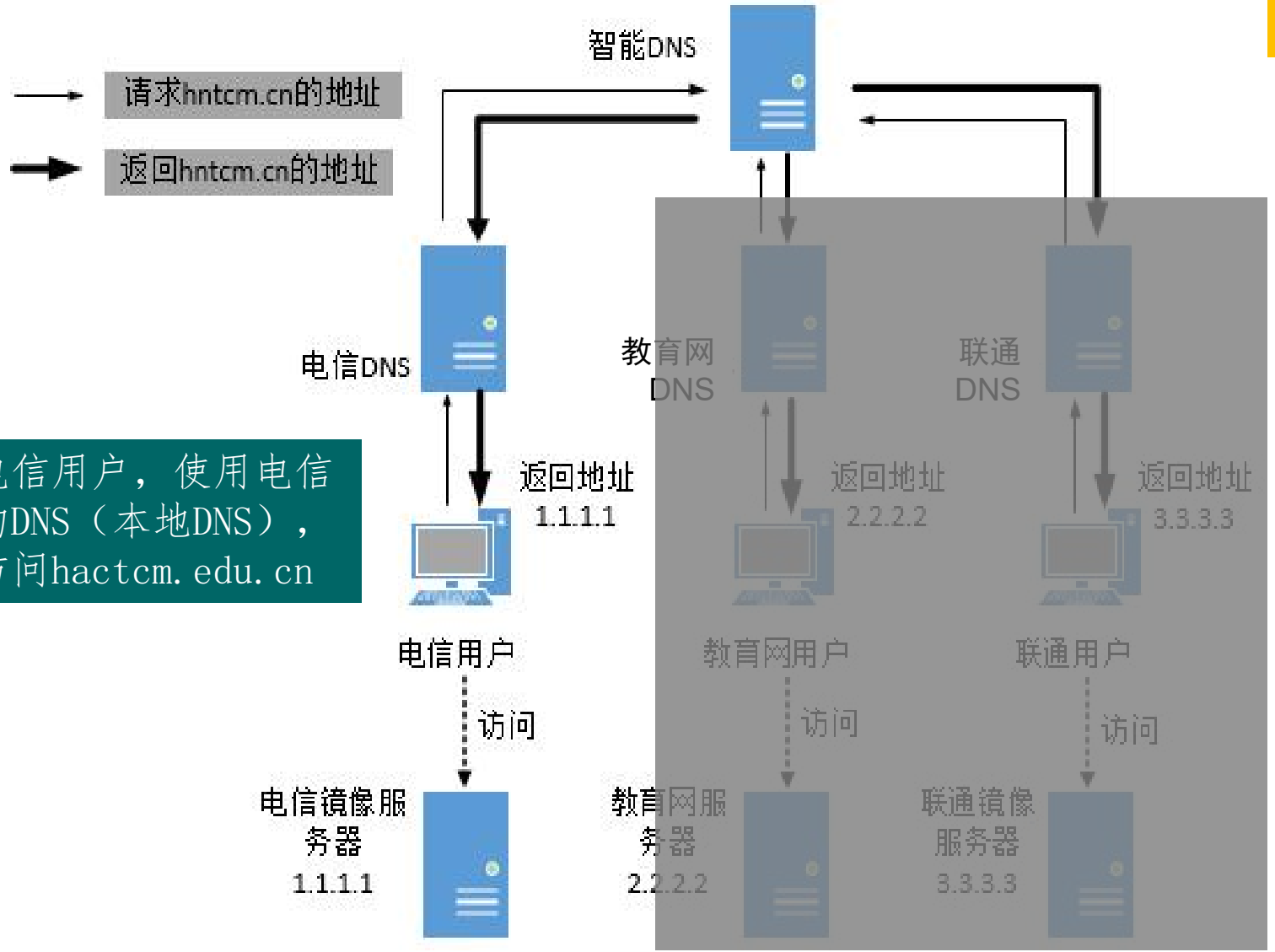

根DNS
权限DNS
网络中心
教育网
本地DNS
跨网
Web服务器
电信网
www.hactcm.edu.cn


根DNS
权限DNS
网络中心
教育网
Web服务器1
本地DNS
Web服务器2
www.hactcm.edu.cn
电信网

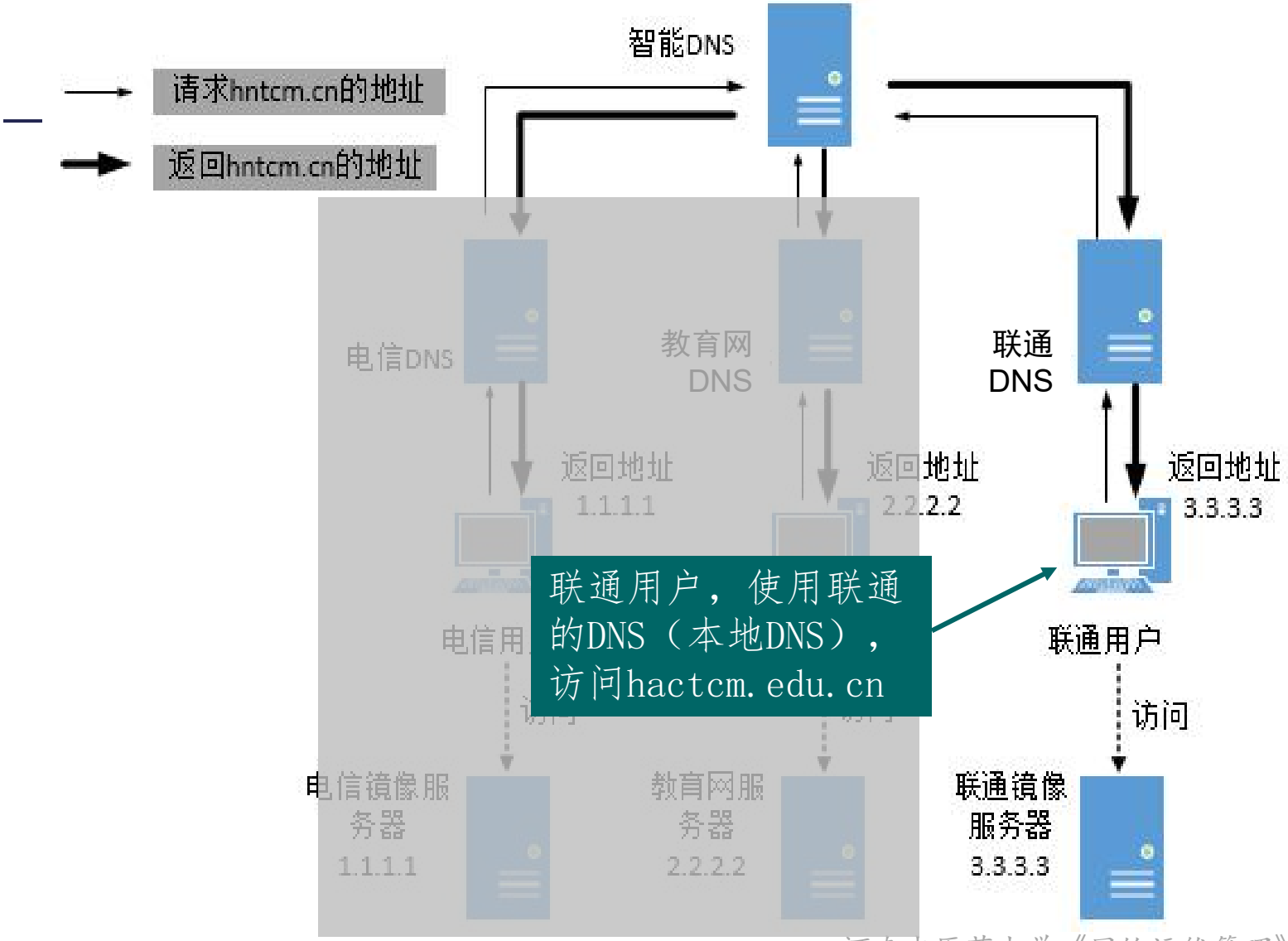
互联网用户访问 www.hactcm.edu.cn

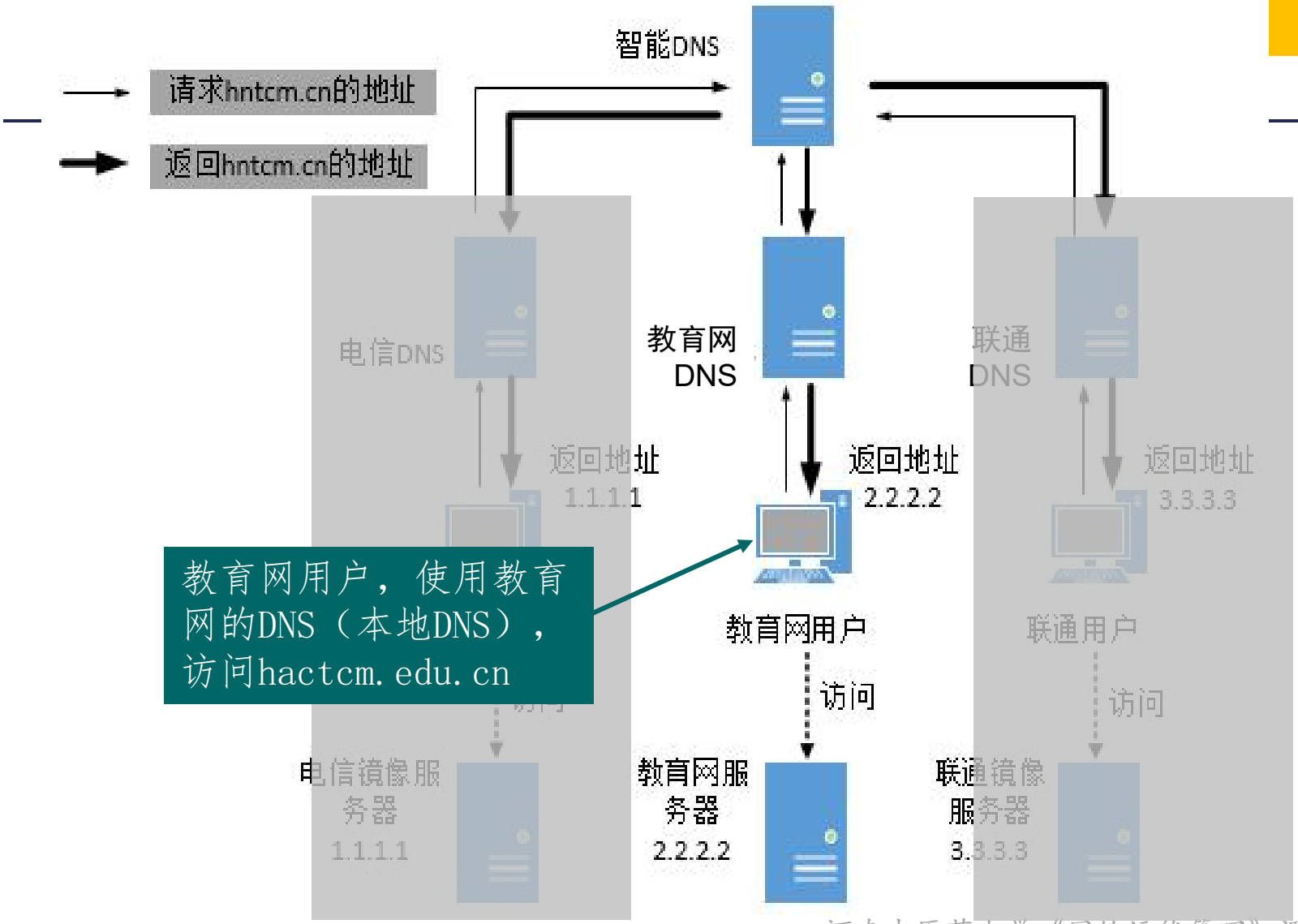
假设：Web服务器除了在教育网内部署之外，又分别在电信网和联通网上部署了镜像服务器，以便于不同网络用户更好地访问河南中医药大学www.hactcm.edu.cn。三台Web服务器的地址如下：


请求hntcm.cn的地址
返回hntcm.cn的地址
智能DNS
电信DNS
教育网
DNS
联通
DNS
返回地址
1.1.1.1
返回地址
2.2.2.2
返回地址
3.3.3.3
电信用户
教育网用户
联通用户
访问
访问
访问
电信镜像服
务器
1.1.1.1
教育网服
务器
2.2.2.2
联通镜像
服务器
3.3.3.3



电信用户，使用电信的DNS（本地DNS），访问hactcm.edu.cn


智能DNS
请求hntcm.cn的地址
返回hntcm.cn的地址
电信DNS
教育网
DNS
联通
DNS
返回地址
1.1.1.1
返回地址
2.2.2.2
返回地址
3.3.3.3
联通用户，使用联通的DNS（本地DNS），访问hactcm.edu.cn
联通用户
访问
电信镜像服务器
1.1.1.1
教育网服务器
2.2.2.2
联通镜像服务器
3.3.3.3


请求hntcm.cn的地址
返回hntcm.cn的地址
智能DNS
电信DNS
教育网
DNS
联通
DNS
返回地址
1.1.1.1
返回地址
2.2.2.2
返回地址
3.3.3.3
教育网用户，使用教育网的DNS（本地DNS），访问hactcm.edu.cn
教育网用户
联通用户
访问
访问
访问
电信镜像服务器
1.1.1.1
教育网服务器
2.2.2.2
联通镜像服务器
3.3.3.3

10. 智能DNS

智能DNS的实现原理

- 定义IP表：定义各个不同客户群的IP表，以区别客户来源。
- 定义智能DNS解析：为每一种不同的客户来源定义一条个性化的DNS解析记录。 使他们之间访问的IP地址不同
- BIND配置：使用BIND来做智能DNS主要使用其View功能。自定义一个IP表，然后通过View功能来进行区别。隶属于IP表A的访问将得到一个地址，隶属于IP表B的将得到另外一个不同的IP地址，但其都对应同一个域名。

配置主配置文件 named.conf

```
options {
directory "/var/named";
pid-file "/tmp/named.pid";
version "Unsupported on this platform";
};
include “cnc.conf” ;
include “edu.conf” ;
view "cnc"{
    match-clients{ CNC;}; //设置匹配本View的客户端, CNC在cnc.conf中有定义;
    recursion no;
    zone "hactcm.edu.cn" IN {
        type master;
        file "cnc.hactcm.edu.cn";
        allow-update { none; };
         };
```

配置主配置文件 named.conf

```
(接上页一一 完)
view "edu"{
match-clients{ EDU;}; //设置匹配本View的客户端，EDU在edu.conf中有定义;
recursion no;
zone "hactcm.edu.cn" IN {
        type master;
        file "edu.hactcm.edu.cn";
        allow-update { none; };
        };
view "any"{
match-clients{any;}; //设置匹配本View的客户端，any指除了CNC和EDU以外的;
recursion no;
zone "hactcm.edu.cn" IN {
        type master;
        file "tel.hactcm.edu.cn";
        allow-update { none; };
        };
```

创建联通用户的IP地址列表文件 cnc.conf

```
# vi /var/named/ cnc.conf
acl "CNC"{
    211.147.208.182/32;
    211.147.208.183/32;
    58.16.0.0/16;
    58.17.0.0/17;
    58.17.128.0/17;
    58.18.0.0/16;
    58.19.0.0/16;
    58.20.0.0/16;
    58.21.0.0/16;
    58.22.0.0/15;
    222.163.128.0/17;
};
```

创建教育网用户的IP地址列表文件 edu.conf

```
# vi /var/named/ edu.conf
acl "EDU"{
    58.154.0.0/15;
    58.192.0.0/15;
    58.194.0.0/15;
    58.196.0.0/15;
    58.198.0.0/15;
    58.200.0.0/13;
    210.25.0.0/16;
    211.83.0.0/16;
    211.84.0.0/15;
    211.86.0.0/15;
    218.192.0.0/16;
};
```

创建联通用户对应的区域配置文件cnc.hactcm.edu.cn

```
# vi /var/named/cnc.hactcm.edu.cn  //以下是区域配置文件cnc.hactcm.edu.cn的内容
$ttl    1H
@       IN SOA  hactcm.edu.cn.  root.hactcm.edu.cn.(
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@               IN      NS      ns1.hntcm.cn.
@               IN      NS      ns2.hntcm.cn.
ns1             IN      A       210.51.170.17
ns2             IN      A       210.51.170.19
www             IN      A       1.1.1.1  //给联通用户返回的IP地址
```

创建教育网用户对应的区域配置文件edu.hactcm.edu.cn

```
# vi /var/named/ edu.hactcm.edu.cn
$ttl    1H
@       IN SOA  hactcm.edu.cn.  root.hactcm.edu.cn.(
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@               IN      NS      ns1.caixun.com.
@               IN      NS      ns2.caixun.com.
ns1             IN      A       210.51.170.17
ns2             IN      A       210.51.170.19
www             IN      A       2.2.2.2  //给教育网用户返回的IP地址
```

创建其他用户对应的区域配置文件 tel.hactcm.edu.cn

```
# vi /var/named/ tel.hactcm.edu.cn
$ttl    1H
@       IN SOA  hactcm.edu.cn. root.hactcm.edu.cn.(
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@        IN       NS       ns1.caixun.com.
@        IN       NS       ns2.caixun.com.
ns1      IN       A        210.51.170.17
ns2      IN       A        210.51.170.19
www      IN       A        3.3.3.3  //给其他用户（非教育、非联通）返回的IP地址
```

10. 智能DNS

智能DNS的优点

- 通过智能DNS，可以有以下应用：
- 镜象网站：在网通及电信的机房放置多个相同的镜象站点， 让不同的地方客户访问不同的站点。
- 负载均衡：对于流量比较大的网站，可以通过该功能把流量分配到几台不同的服务器上，以提高网站的运行速度。
- 个性化站点服务：比如通过IP表的重新定义， 让国外的客户自动访问英文版的网站； 让国内的客户自动访问中文版的网站。

10. 智能DNS

能DNS也有不足

- 智能dns的自动寻路功能的关键在于提供的ip段列表和向智能dns发起询问的机器的ip地址。通过这2个因素判断，进而返回不同ip地址。但是在此机制下会产生一种问题，就是如果网通用户自己本身的client设定的dns是电信的dns，那么网通用户得到的地址也将是电信的地址，这个智能dns无法进行有效判断。

第3讲

完